

Country Reports

Afghanistan

Afghanistan is not a regional financial or banking center, and is not considered an offshore financial center. However, its formal financial system is growing rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan is a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. Afghanistan passed anti-money laundering and terrorist financing legislation in October 2005, and efforts are being made to strengthen police and customs forces. However, there remain few resources, limited capacity, little expertise and insufficient political will to combat financial crimes. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector. Public corruption is a significant problem. Afghanistan is ranked 172 out of 180 countries in Transparency International's 2007 Corruption Perception Index.

According to United Nations (UN) statistics, in 2005 and 2006, opium production increased and today Afghanistan accounts for over 90 percent of the world's opium production. Opium gum is sometimes used as a currency—especially by rural farmers—and it is used as a store of value in prime production areas. It is estimated that at least one third of Afghanistan's (licit plus illicit) gross domestic product (GDP) is derived directly from narcotics activities, and proceeds generated from the drug trade have reportedly fueled a growing real estate boom in Kabul, as well as a sharp increase in capital investment in rural poppy growing areas.

Much of the recent rise in opium production comes from Taliban strongholds in the southern part of the country. The Taliban impose taxes on narcotics dealers, which undoubtedly helps finance their terrorist activities. Additional revenue streams for the Taliban and regional warlords come from "protecting" opium shipments, running heroin labs, and from "toll booths" established on transport and smuggling routes.

Afghan opium is refined into heroin by production labs, more of which are being established within Afghanistan's borders. The heroin is then often broken into small shipments and smuggled across porous borders for resale abroad. Payment for the narcotics outside the country is facilitated through a variety of means, including through conventional trade and the traditional hawala system that uses trade as the primary medium to balance accounts. In addition, the narcotics themselves are often used as tradable goods and as a means of exchange for automobiles, construction materials, foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan and Iran. Many of these goods are smuggled into Afghanistan from neighboring countries, particularly Iran and Pakistan, or enter via the Afghan Transit Trade Agreement (ATTA) without payment of customs duties or tariffs. Most of the trade goods imported into Afghanistan originate in Dubai. Invoice fraud, corruption, indigenous smuggling networks, underground finance, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and nonfinancial business services in local, regional, and international markets. Financial activities include foreign exchange transactions, funds transfers (particularly to and from neighboring countries with weak regulatory regimes for informal remittance systems), micro and trade finance, as well as some deposit-taking activities. While the hawala network may not provide financial intermediation of the same type as the formal banking system (i.e., deposit-taking for lending and investing purposes based on the assessment, underwriting, and pricing of risks), it is a traditional form of finance and deeply entrenched and widely used throughout Afghanistan and the neighboring region.

There are over 300 known hawala dealers in Kabul, with branches or additional dealers in each of the 34 provinces. These dealers are organized into informal provincial unions or guilds whose members maintain a number of agent-principal and partnership relationships with other dealers throughout the country and internationally. Their record keeping and accounting practices are robust, efficient, and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are supposed to be licensed; however the licensing regime that existed from April 2004 until September of 2006 was overly burdensome and resulted in issuance of few licenses. In September of 2006, Da Afghanistan Bank (DAB), Afghanistan's Central Bank, issued a new money service provider regulation that streamlined the licensing process and substantially reduced the licensing and ongoing compliance burden for hawaladars. The focus of the regulation is on anti-money laundering and counter-terrorist financing (AML/CTF). The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. The DAB provided training sessions on the regulation and has developed a streamlined application process. In Kabul, approximately 100 licenses have been issued under the regulation, which is the result of the DAB outreach, law enforcement actions, and pressure from commercial banks where hawaladars hold accounts. Options for strengthening the hawaladar unions and promoting self-regulation are also being studied. The DAB has begun outreach efforts to money service providers in other large cities, specifically Mazar-e-Sharif and Herat, and hopes to expand the licensing to these cities in 2008. Given how widely used the hawala system is in Afghanistan, financial crimes undoubtedly occur through these entities.

In early 2004, the DAB worked in collaboration with international donors to establish the legislative framework for AML/CTF initiatives. Although Afghanistan was unable to meet its initial commitment to enact both pieces of legislation by September 30, 2004, they were both finalized and signed into law by late October 2004.

The Anti-Money Laundering and Proceeds of Crime and Combating the Financing of Terrorism laws incorporate provisions that are designed to meet the recommendations of the Financial Action Task Force (FATF). These laws address the criminalization of money laundering and the financing of terrorism, customer due diligence, the establishment of a financial intelligence unit (FIU), international cooperation, extradition, and the freezing and confiscation of funds. Under the law, money laundering and terrorist financing are criminal offences. The AML law also includes provisions to address cross-border currency reporting, and establishes authorities to seize and confiscate monies found to be undeclared or falsely declared, or determined to be transferred for illicit purposes.

Under the AML law, the Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA), Afghanistan's FIU, has been established and is functioning as a semi-autonomous unit within the DAB. The FIU, originally to be established in January 2005, was actually initiated in October 2005—with the assignment of a General Director, office space, and other basic resources.

Banks and other financial and nonfinancial institutions are required to report to the FIU all suspicious transactions and large cash transactions above the equivalent of U.S. \$10,000, as prescribed by the DAB. These financial institutions are also required to maintain their records for a minimum of 10 years. Approximately 10,000 large cash transaction reports are currently being received from financial institutions and processed each month. The FIU has over 140,000 large transaction reports currently stored in its database that can be searched using a number of criteria. The FIU has the legal authority to freeze financial assets for up to seven days. FinTRACA also has access to records and databases of other government entities.

The formal banking sector consists of sixteen licensed banks. AML examinations have been conducted for all these banks that have resulted in a growing awareness of AML requirements, deficiencies among the banks, and a need for building the AML capacity of the formal financial sector. Additionally, the Central Bank has worked with the banking community through the Afghan Bankers

Association (ABA) to develop several ongoing topical working groups focused on AML issues. The ABA has recently designed a “know your customer” (KYC) form that has been accepted by the financial industry and has provided on-going education on identifying suspicious transactions. Seven suspicious transaction reports were received in 2007 by the FIU, one of which was referred to law enforcement for investigation.

The Afghanistan Central Bank has circulated a list of individuals and entities that have been included on the UN 1267 Sanctions Committee’s consolidated list of designated individuals and entities to financial institutions. There is no information currently available regarding the results of these lists being circulated.

The Supervision Department within the DAB was formed at the end of 2003, and is divided into four divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), and Regulation. The Department is charged with administering the AML/CTF legislation, conducting examinations, licensing new institutions, overseeing money service providers, and outreach to the commercial banking sector. The effectiveness of the Supervision Department in the AML area remains limited due to staffing, organization, and management issues. As a result, FinTRACA has taken on some supervisory responsibilities, yet resources are limited.

The Ministry of Interior (MOI) and the Attorney General’s Office are the primary financial enforcement and investigative authorities. They are responsible for tracing, seizing and freezing assets. While MOI generally has adequate police powers, it lacks the resources to trace, seize, and freeze assets. According to FinTRACA, it is not aware of Afghanistan freezing, seizing, or forfeiting related assets in 2007, or of any calls on the banking community for cooperation with enforcement efforts. FinTRACA has an MOU in place with the MOI for cooperation and currently shares information with the Sensitive Investigations Unit (SIU), a law enforcement group within the MOI.

Pursuant to the Central Bank law, a Financial Services Tribunal will be established to review certain decisions and orders of the DAB. Judges and administrative staff will need to significantly increase their technical knowledge before the Tribunal is effective. The Tribunal will review supervisory actions of the DAB, but will not prosecute cases of financial crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court, where there has been little to no activity in the last three years. The process to prosecute and adjudicate cases is long and cumbersome, significantly underdeveloped, and corruption can play a role at various levels. There was one arrest for alleged terrorist financing in 2007 but the individual was not prosecuted.

Border security continues to be a major issue throughout Afghanistan. At present there are 21 border crossings that have come under central government control, utilizing international donor assistance as well as local and international forces. However, many of the border areas are not policed and therefore susceptible to illicit cross-border trafficking and trade-based money laundering. Many regional warlords also continue to control the international borders in their provincial areas, causing major security risks. Customs authorities, with the help of outside assistance, have made significant strides, but much work remains to be done.

Customs collection has improved, but smuggling and corruption continue to be major concerns, as well as trade fraud, which includes false and over-and under-invoicing. Thorough cargo inspections are not conducted at any gateway. A pilot program for declaring large, cross-border currency transactions has been developed at the Kabul International Airport (KIA). This prototype will serve as the foundation for expansion to other land, air and sea crossings. Currently, KIA requires incoming and outgoing passengers to fill out declarations forms for carrying cash in an amount of 1 million Afghanis (approximately U.S. \$20,000) or its equivalent. The DAB is working with Customs authorities to further improve enforcement of airport declarations. However there is very little international air travel outside of Kabul. Although Afghanistan has limited resources to enforce

customs declarations outside of Kabul, the DAB has sent delegations to border crossings in Hairatan and Islam Qala to assess the capacity and describe the provisions of the law to the local authorities. There is no restriction on transporting any amount of declared currency. However, in the case of cash smuggling at the airport, reports are entered into a Customs database and this information is shared with the FIU.

Under the Law on Combating the Financing of Terrorism, any nonprofit organization that wishes to collect, receive, grant, or transfer funds and property must be entered in the registry with the Ministry of Auqaf (Islamic Affairs). All nonprofit organizations are subject to a due diligence process which includes an assessment of accounting, record keeping, and other activities. However, the capacity of the Ministry to conduct such examinations is nearly nonexistent, and the reality is that any organization applying for a registration is granted one. Furthermore, because no adequate enforcement authority exists, many organizations operating under a “tax-exempt” nonprofit status in Afghanistan go completely unregistered, and illicit activities are suspected on the part of a number of organizations.

The Government of Afghanistan (GOA) is a party to 12 of the United Nations (UN) conventions and protocols against terrorism and is a signatory to the International Convention for the Suppression of Acts of Nuclear Terrorism (which is pending ratification). Afghanistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Afghanistan is also a signatory to the UN Convention against Corruption (UNCAC). Ratification of UNCAC, one of the benchmarks established under the London Compact, as well as amendment of domestic laws to conform to the UNCAC’s obligations, remain pending.

In July 2006, Afghanistan became a member in the Asia Pacific Group, a FATF-Style Regional Body (FSRB), and has also obtained observer status in the Eurasian Group, another FSRB. No mutual evaluation has been conducted on the AML/CTF regime of Afghanistan to date; however, the APG is scheduled to assess the financial system in the third quarter of 2009. FinTRACA, Afghanistan’s FIU, has active bilateral MOUs for cooperation with the FIU’s of the United Kingdom, Russia, the Kyrgyz Republic, and Belarus. Although FinTRACA is not yet a member of the Egmont Group of financial intelligence units, it has taken several steps to build its capacity in efforts to meet international standards.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Improvement has been seen in development of its nascent FIU, the reporting of large cash transactions, participation in international AML bodies, improvement in bank AML compliance awareness, information technology systems, and in efforts to bring money service providers into a legal and regulatory framework. However, much work remains to be done. Afghanistan needs to commit additional resources and find the political will to seriously combat financial crimes, including corruption. Afghanistan should develop secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should develop the investigative capabilities of law enforcement authorities in the various areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities need to become proficient in understanding the various elements required for money laundering prosecutions. The FIU should become autonomous and increase its staff and resources. Afghan customs authorities should implement cross-border currency reporting and learn to recognize forms of trade-based money laundering. Border enforcement should be a priority, both to enhance scarce revenue and to disrupt narcotics trafficking and illicit value transfer. Afghan authorities should also work to address the widespread corruption in commerce and government.

Albania

Albania is not considered an important regional financial or offshore center. As a transit country for trafficking in narcotics, arms, contraband, and humans, Albania remains at significant risk for money laundering. The major sources of criminal proceeds in the country are trafficking offenses, official corruption and fraud. Corruption and organized crime are likely the most significant sources of money laundering, but the exact extent to which these various illegal activities contribute to overall crime proceeds and money laundering is unknown.

Criminals frequently invest tainted money in real estate and business development projects. Albania has a significant black market for smuggled goods because of its high level of consumer imports and weak customs controls. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries and often return their illicit gains to Albania. The proceeds from these activities are easily laundered in Albania because of the cash economy and weak government controls on banking.

As a cash-based economy, the Albanian economy is also particularly vulnerable to money laundering activity. Few individuals have bank accounts and check writing is not common. Of the 17 banks in Albania, five of them are considered to have a significant national presence. According to the Bank of Albania (the Central Bank), 25 percent of the money in circulation is outside of the banking system, compared to an average of 10 percent in other Central and Eastern European transitioning economies. A significant portion of remittances enters the country through unofficial channels. It is estimated that only half of total remittances enter Albania through banks or money transfer companies. According to a 2007 United Nations Office on Drugs and Crime (UNODC) report, remittances comprise nearly 14 percent of Albania's annual gross domestic product (GDP.) Black market exchange is still present in the country despite repeated efforts by the Government of Albania (GOA) institutions to impede such exchanges. The Bankers Association estimates that only 20-30 percent of transactions take place through formal banking channels. Similarly, the GOA estimates that proceeds from the informal sector account for approximately 30-60 percent of Albania's GDP. Although current law permits the operation of free trade zones, none are currently in operation.

Electronic and automatic teller machine (ATM) transactions are relatively few in number but are growing as more banks introduce this technology. The number of ATMs expanded following the decision of the GOA to deliver salaries through electronic transfers. All central government institutions have now converted to electronic pay systems, and many private companies have also started to issue salaries electronically. Credit card usage has also increased, but only a small number of people possess them and usage is primarily limited to a few large vendors. Bank fraud still remains largely undetected.

Albania criminalized money laundering with Article 287, Albanian Criminal Code 1995, as amended. Albania's original money laundering law was "On the Prevention of Money Laundering", or Law No. 8610 of 17 May 2000. In June 2003, Parliament approved Law No. 9084, which strengthened the old Law No. 8610, and improved the Criminal Code and the Criminal Procedure Code. The new law redefined the legal concept of money laundering, harmonizing the Albanian definition with that of the European Union (EU) and international conventions. Under the revised Criminal Code, Albania expanded and upgraded many powers. The new law also revises the definition of money laundering, outlaws the establishment of anonymous accounts, and permits the confiscation of accounts. The law also mandates the identification of beneficial owners. Currently, no law criminalizes negligence by financial institutions in money laundering cases. The Bank of Albania has established a task force to confirm banks' compliance with customer verification rules.

Albania's law sets forth an "all crimes" definition for the offense of money laundering. However, the Albanian court system applies a difficult burden of proof. Albanian courts require a prior or simultaneous conviction for the predicate offense before issuing an indictment for money laundering.

Law 9084 places reporting requirements on both financial institutions and individuals. Obligated institutions must report to Albania's financial intelligence unit (FIU) all transactions that exceed approximately U.S. \$200,000 as well as those transactions that involve suspicious activity, regardless of the amount. A new draft law, when enacted, will lower the threshold for currency transaction reporting from the current U.S. \$200,000 to U.S. \$15,000, thereby ensuring compliance with EU standards. Subject transactions must be reported within 72 hours of their occurrence. Individuals and entities reporting transactions are protected by law if they cooperate with and provide financial information to the FIU and law enforcement agencies. Reportedly, however, leaks of financial disclosure information from other agencies compromise the entities' client confidentiality.

Under current Albanian law, financial institutions have no legal obligation to identify customers prior to opening an account. Albania distinguishes between record keeping of client information and record keeping of transaction information, and, in an effort to reduce the record-keeping burden on obligated entities, has a different threshold for each. While most banks have internal rules mandating customer identification, Albania's money laundering law only requires customer identification prior to conducting transactions that exceed approximately U.S. \$20,000 or when there is a suspicion of money laundering. For all transactions in excess of U.S. \$20,000, entities must maintain customer records. With regard to transactions, obliged entities are not required to maintain records on transactions under a U.S. \$200,000 threshold. For every transaction in excess of U.S. \$200,000 entities must maintain records that can be used to reconstruct the transaction if necessary. If there is no suspicion, entities must retain customer identification information for all transactions exceeding U.S. \$20,000—but could destroy all records of financial transactions below U.S. \$200,000. The new draft law, when enacted, will require client identification regardless of the size of the transaction.

It is the responsibility of the licensing authority to supervise intermediaries for compliance. For example, the Ministry of Justice is responsible for oversight of attorneys and notaries, and the Ministry of Finance for accountants. Although regulations also cover nonbank financial institutions, enforcement has been poor in practice. There is an increasing number of suspicious transaction reports (STRs) coming from banks as that sector matures, although the majority continues to come from tax and customs authorities and foreign counterparts.

Individuals must report to customs authorities all cross-border transactions that exceed approximately U.S. \$10,000. Albania provides declaration forms at border crossing points, and the law does not distinguish between an Albanian and a foreign visitor. However, customs controls on cross-border transactions lack effectiveness due to a lack of resources, poor training and, reportedly, corruption of customs officials.

Law No. 8610 established an administrative FIU to coordinate the GOA's efforts to detect and prevent money laundering. Under Law No. 9084, the FIU became a quasi-independent agency within the Ministry of Finance, formally known as the General Directorate for the Prevention of Money Laundering (DPPPP). Albania is in the process of preparing a new administrative law on FIU operations. Referred to as the "draft law," it will clarify certain anti-money laundering measures and elaborate on reporting requirements for obliged entities.

As an administrative-type FIU, the DPPPP does not have law enforcement capabilities. The FIU receives reports from obliged entities, analyzes them, and then disseminates the results of its analysis to the prosecutor's office. After nearly six years, the FIU cannot demonstrate any referral that has resulted in a money laundering prosecution. There were only three money laundering referrals to the Prosecutor's Office during 2006 and all three were declined for prosecution. There were no money laundering referrals to the Prosecutor's Office during 2007. In an effort to increase money laundering prosecutions, in May 2007, Albania established the Economic Crimes and Corruption Joint Investigative Unit (ECCJIU) within the Tirana District Prosecution Office. This unit focuses efforts and builds expertise in the investigation and prosecution of financial crimes and corruption cases by

bringing together members of the General Prosecutors Office, the Albanian State Police's Financial Crimes Sector, the Ministry of Finance's Customs Service and Tax Police, and Albanian intelligence services. The ECCJIU will also receive cooperation from the FIU and the National Intelligence Service. The ECCJIU will have responsibility for the prosecution of money laundering cases within the District of Tirana.

To address the criminal aspects of its informal economy, Albania passed comprehensive legislation against organized crime in 2004. Law No. 9284, the "anti-mafia law," enables civil asset sequestration and confiscation provisions in cases involving organized crime and trafficking. The law applies to the assets of suspected persons, their families, and close associates. In cases where the value of the defendant's assets exceeds the income generated by known legal activity, the law places the burden on the defendant to prove a legitimate source of income for the assets. During 2006, the Serious Crimes Prosecution Office filed twenty forfeiture cases pursuant to the anti-mafia law. The properties sequestered include a sports center of 4000 square meters, hotels, apartments, land, vehicles, and approximately U.S. \$35,000 in cash. Although the Agency for the Administration of the Sequestration and Confiscation of Assets (AASCA) is charged with the responsibility of administering confiscated assets, the agency has failed to function in a meaningful fashion. As such, enforcement of the assets law remains reportedly inadequate due to a lack of financial or political support for the agency.

Article 230/a of the Penal Code criminalizes the financing of terrorism. Financing of terrorism or its support of any kind is punishable by a term of imprisonment of at least fifteen years, and carries a fine of U.S. \$50,000 to U.S. \$100,000. The Penal Code also contains additional provisions dealing with terrorist financing including sections dealing with giving information regarding the investigation or identification to identified persons, and conducting financial transactions with identified persons. There are no known prosecutions under these laws, but the Prosecutor's Office is currently investigating one case with such implications.

In 2004, Albania enacted Law No. 9258, "On Measures against Terrorist Financing". This law provides a mechanism for the sequestration and confiscation of assets belonging to terrorism financiers, particularly as to the United Nations (UN) updated lists of designees. While comprehensive, it lacks implementing regulations and thus is not fully in force. As of October 2007, the Ministry of Finance claimed to maintain asset freezes against six individuals and fourteen foundations and companies from the UN Security Council's 1267 Consolidated lists of identified terrorist entities. In total, assets worth more than U.S. \$10 million, belonging to six persons, five foundations and nine companies, remain sequestered. Reportedly, the full extent of sequestered assets and their exact whereabouts are unknown.

The Ministry of Finance is the main entity responsible for issuing freeze orders. After the Minister of Finance executes an order, the FIU circulates it to other government agencies, which then sequester any assets found belonging to the UNSCR 1267 named individual or entity. The sequestration orders remain in force as long as their names remain on the list.

Albania is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the 1988 UN Drug Convention. Albania is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and was most recently evaluated by MONEYVAL in July 2006. Albania's FIU is also a member of the Egmont Group, the international organization of financial intelligence units.

Although there are continuing initiatives to improve Albania's capacity to deal with financial crimes and money laundering, the lack of positive results and apparent inability to adequately address the deficiencies in the programs continue to hamper progress. Despite Albania's efforts, additional improvements are needed. Albania should increase support and training for the FIU, as a majority of its staff is new and lacks experience in the analysis of money laundering and terrorist financing cases.

The FIU should create or obtain a database to allow effective analysis of the large volume of currency transaction reports and suspicious transaction reports received. Albania should ensure that those charged with pursuing financial crime increase their technical knowledge to include modern financial investigation techniques. Albania should provide its police force with a central database. Investigators and prosecutors should implement case management techniques, and prosecutors, and judges need to become more conversant with the nuances of money laundering. The FIU, prosecutors and ECCJIU should enhance their effectiveness through cooperation with one another and outreach to other entities. Albania should remove the requirement of a conviction for the predicate offense before a conviction for money laundering can be obtained. Albania should devise implementing regulations for Law 9258 regarding sequestration and confiscation of assets linked to the financing of terrorism so that it can be fully effective. The Government of Albania should also improve the enforcement and enlarge the scope of its asset seizure and forfeiture regime, including fully funding and supporting the Agency for the Administration of the Sequestration and Confiscation of Assets (AASCA). Albania should also incorporate into anti-money laundering legislation specific provisions regarding negligent money laundering, corporate criminal liability, comprehensive customer identification procedures, and the adequate oversight of money remitters and charities. Albania should enact its draft law and promulgate implementing regulations as soon as possible.

Algeria

Algeria is not a regional financial center or an offshore financial center. The extent of money laundering through formal financial institutions is thought to be minimal due to stringent exchange control regulations and an antiquated banking sector. The partial convertibility of the Algerian dinar enables the Bank of Algeria (Algeria's Central Bank) to monitor all international financial operations carried out by public and private banking institutions. Embezzlement, fraud, and tax evasion are common financial crimes. Algeria has a large informal and cash-based economy. Algeria is a transit country for men and women trafficked from sub-Saharan Africa en route to Europe.

Algeria first criminalized terrorist financing through the adoption of Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by five to ten years of imprisonment. On February 5, 2005, Algeria enacted public law 05.01, entitled "The Prevention and Fight against Money Laundering and Financing of Terrorism." The law aims to strengthen the powers of the Cellule du Traitement du Renseignement Financier (CTRF), an independent financial intelligence unit (FIU) within the Ministry of Finance (MOF) created in 2002. This law seeks to bring Algerian law into conformity with international standards and conventions. It offers guidance for the prevention and detection of money laundering and terrorist financing, institutional and judicial cooperation, and penal provisions.

The 2005 legislation extends money laundering controls to specific, nonbank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided that information is shared with CTRF in good faith, the law offers immunity from administrative or civil penalties for individuals who cooperate with money laundering and terrorist finance investigations. Under the law, assets may be frozen for up to 72 hours on the basis of suspicious activity; such freezes can only be extended with judicial authorization. Financial penalties for noncompliance range from 50,000 to 5 million Algerian dinars (approximately U.S. \$760 to U.S. \$76,000). In addition to its provisions pertaining to money laundered from illicit activities, the law allows the investigation of terrorist-associated funds derived from "clean" sources.

The law provides significant authority to the Algerian Banking Commission, the independent body established under the authority of the Bank of Algeria to supervise banks and financial institutions, to inform CTRF of suspicious or complex transactions. The law also gives the Algerian Banking Commission, CTRF, and the Algerian judiciary wide latitude to exchange information with their

foreign government counterparts in the course of money laundering and terrorist finance investigations, provided confidentiality for suspected entities is insured. A clause excludes the sharing of information with foreign governments in the event legal proceedings are already underway in Algeria against the suspected entity, or if the information is deemed too sensitive for national security reasons.

On November 14, 2005, the Government of Algeria issued Executive Decree 05-442 establishing a deadline of September 1, 2006 after which all payments in excess of 50,000 Algerian dinars must be made by check, wire transfer, payment card, bill of exchange, promissory note, or other official bank payment. While nonresidents are exempt from this requirement, they must (like all travelers to and from the country) report foreign currency in their possession to the Algerian Customs Authority. The government suspended the deadline in September 2006, however, in response to the slow implementation of a nation-wide electronic check-clearing system that failed to gain the confidence of the Algerian business community.

In 1996 Algeria adopted ordinance 96-22 regarding exchange regulations and currency movements abroad. The law criminalized cash smuggling as well as the failure to respect reporting requirements for the transfer of cash into or out of Algeria. The maximum value of cash that may be carried by an individual at any given time is the equivalent of 7,600 euros (approximately U.S. \$11,000). Higher sums may only be legally sent abroad by wire transfer. Given limits on convertibility of the Algerian dinar, even sums less than the 7,600 euros threshold must be accompanied by a bank statement declaring that the holder acquired the foreign currency with the authorization of the central bank. Holders of foreign currency without such a declaration, such as individuals who traded dinars for foreign currencies in one of Algiers' many black markets, risk confiscation. In addition to foreign currency, the ordinance applies to other liquid financial instruments, precious metals and gemstones. Penalties for noncompliance range from three to five years of imprisonment or a fine valued of up to twice the value of the seized property.

Algerian financial institutions, as well as Algerian customs and tax administration agents, are required to report any activities they suspect of being linked to criminal activity, money laundering, or terrorist financing to CTRF and comply with subsequent CTRF inquiries. They are obligated to verify the identity of their customers or their registered agents before opening an account; they must furthermore record the origin and destination of funds they deem suspicious. In addition, these institutions must maintain confidential reports of suspicious transactions and customer records for at least five years after the date of the last transaction or the closing of an account.

In 2006, the Algerian customs service reported 373 cases of cash smuggling with a total value of U.S. \$5.6 million. These cases occurred in 11 of the country's 48 wilayas (regional departments). In 2005, customs reported 426 cases with a total value of U.S. \$2.7 million. The total fines levied against smugglers were U.S. \$41 million in 2006. In 2007, CTRF investigated 103 suspicious transaction reports.

The Ministry of Interior is charged with registering foreign and domestic nongovernmental organizations in Algeria. While the Ministry of Religious Affairs legally controls the collection of funds at mosques for charitable purposes, some of these funds escape the notice of government monitoring efforts.

Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. In response, Algerian authorities are taking steps to coordinate information sharing between concerned agencies.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN

Convention against Corruption, and the 1988 UN Drug Convention. In addition, Algeria is a signatory to various UN, Arab, and African conventions against terrorism, trafficking in persons, and organized crime. The Ministry of Justice is expected to create a pool of judges trained in financial matters.

The Government of Algeria has taken significant steps to enhance its statutory regime against money laundering and terrorist financing. It needs to move forward now to implement those laws and eliminate bureaucratic barriers among various government agencies by empowering CTRF to be the focal point for the AML/CTF investigations. In addition, given the scope of Algeria's informal economy, it should renew its initiative to limit the size of cash transactions. Algerian law enforcement and customs authorities need to enhance their ability to recognize and investigate trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

Angola

Angola is neither a regional nor an offshore financial center and has not prosecuted any known cases of money laundering. Angola does not produce significant quantities of drugs, although it continues to be a transit point for drug trafficking, particularly cocaine brought in from Brazil or South Africa destined for Europe. The laundering of funds derived from continuous and widespread high-level corruption is a concern, as is the use of diamonds as a vehicle for money laundering. The Government of the Republic of Angola (GRA) has implemented a diamond control system in accordance with the Kimberley Process. However, corruption and Angola's long and porous borders further facilitate smuggling and the laundering of diamonds.

Angola currently has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crimes. Other provisions of the criminal code do address some related crimes. The various ministries with responsibility for detection and enforcement are revising a draft anti-money laundering law drawn up with help from the World Bank. The Central Bank's Supervision Division, which has responsibility for money laundering issues, exercises some authority to detect and suppress illicit banking activities under legislation governing foreign exchange controls. The Central Bank has the authority to freeze assets, but Angola does not presently have an effective system for identifying, tracing, or seizing assets. Instead, such crimes are addressed through other provisions of the criminal code. For example, Angola's counternarcotics laws criminalize money laundering related to narcotics trafficking.

Angola's high rate of cash flow makes its financial system an attractive site for money laundering. With no domestic interbank dollar clearing system, even dollar transfers between domestic Angolan banks are logged as "international" transfers, thus creating an incentive to settle transfers in cash. The local banking system imports approximately U.S. \$200-300 million in currency per month, largely in dollars, without a corresponding cash outflow. Local bank representatives have reported that clients have walked into banks with up to U.S. \$2 million in a briefcase to make a deposit. No currency transaction reports cover such large cash transactions. These massive cash flows occur in a banking system ill-equipped to detect and report suspicious activity. The Central Bank has no workable data management system and only rudimentary analytic capability. Corruption pervades Angolan society and commerce and extends across all levels of government. Angola is rated 147 out of 180 countries in Transparency International's 2007 International Corruption Perception Index.

Angola is party to the 1988 UN Drug Convention and the UN Convention against Corruption. Angola has signed but has not yet ratified the UN Convention against Transnational Organized Crime. Angola has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Angola should pass its pending legislation to criminalize money laundering beyond drug offenses and terrorist financing. The GRA should establish a system of financial

transparency reporting requirements and a corresponding Financial Intelligence Unit through legislation that adheres to world standards. The GRA should then move quickly to implement this legislation and bolster the capacity of law enforcement to investigate financial crimes. Angola's judiciary, including its Audit Court (Tribunal de Contas) should give priority to prosecuting financial crimes, including corruption. The GRA should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The GRA should increase efforts to combat official corruption, by establishing an effective system to identify, trace, seize, and forfeit assets and by empowering investigative magistrates to actively seek out and prosecute high profile cases of corruption.

Antigua and Barbuda

Antigua and Barbuda has comprehensive legislation in place to regulate its financial sector, but remains susceptible to money laundering because of its offshore financial sectors and Internet gaming industry. As with other countries in the region, illicit proceeds from the transshipment of narcotics are laundered in Antigua and Barbuda. Its offshore financial sector exacerbates Antigua and Barbuda's vulnerability to money laundering.

In 2007, Antigua and Barbuda had 17 offshore banks, three offshore trusts, two offshore insurance companies, 3,255 international business corporations (IBCs), and 23 licensed Internet gaming companies. The International Business Corporations Act of 1982 (IBCA), as amended, is the governing legal framework for offshore businesses in Antigua and Barbuda. Bearer shares are permitted for international companies. However, the license application requires disclosure of the names and addresses of directors (who must be natural persons), the activities the corporation intends to conduct, the names of shareholders, and number of shares they will hold. Registered agents or service providers are required by law to know the names of beneficial owners. Failure to provide information or giving false information is punishable by a fine of U.S. \$50,000. Offshore financial institutions are exempt from corporate income tax. All licensed institutions are required to have a physical presence, which means presence of at least a full-time senior officer and availability of all files and records. Shell companies are not permitted.

Antigua and Barbuda has five domestic casinos, which are required to incorporate as domestic corporations. Internet gaming companies are required to incorporate as IBCs, and as such are required to have a physical presence. Internet gaming sites are considered to have a physical presence when the primary servers and the key person are resident in Antigua and Barbuda. The Government of Antigua and Barbuda (GOAB) receives approximately U.S. \$2.8 million per year from license fees and other charges related to the Internet gaming industry. A nominal free trade zone in the country seeks to attract investment in priority areas of the government. Casinos and sports book-wagering operations in Antigua and Barbuda's free trade zone are supervised by the Office of National Drug Control and Money Laundering Policy (ONDCP), which serves as the GOAB's financial intelligence unit (FIU), and the Directorate of Offshore Gaming (DOG), housed in the Financial Services Regulatory Commission (FSRC). The GOAB has adopted regulations for the licensing of interactive gaming and wagering, to address possible money laundering through client accounts of Internet gambling operations. The FSRC and DOG have also issued Internet gaming technical standards and guidelines. Internet gaming companies are required to submit quarterly and annual audited financial statements, enforce know-your-customer verification procedures, and maintain records relating to all gaming and financial transactions of each customer for six years. Suspicious activity reports from domestic and offshore gaming entities are sent to the ONDCP and FSRC.

The GOAB has not initiated a unified regulatory structure or uniform supervisory practices for its domestic and offshore banking sectors. Currently, the Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. The Registrar of Insurance supervises and

examines domestic insurance agencies. The director of the ONDCP—who was designated in 2003 as the Supervisory Authority created under the Money Laundering Prevention Act of 1996 (MLPA)—supervises all financial institutions for compliance with suspicious transaction reporting requirements. The FSRC is responsible for the regulation and supervision of all institutions licensed under the IBCA, including offshore banking and all aspects of offshore gaming. This includes issuing licenses for IBCs, maintaining the register of all corporations, and conducting examinations and reviews of offshore financial institutions as well as some domestic financial entities, such as insurance companies and trusts.

In the offshore sector, the IBCA requires that a corporate entity submit all books, minutes, cash, securities, vouchers, customer identification, and customer account records. Financial institutions are required to maintain records for six years after an account is closed. The IBCA provides for disclosure of confidential information pursuant to a request by the director of the ONDCP, and pursuant to an order of a court of competent jurisdiction in Antigua and Barbuda. In addition, section 25 of the MLPA states that the provisions of this Act shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any law or otherwise. The MLPA contains provisions for obtaining client and ownership information.

The MLPA, as amended, is the cornerstone of Antigua and Barbuda's anti-money laundering legislation. The MLPA makes it an offense for any person to obtain, conceal, retain, manage, or invest illicit proceeds or bring such proceeds into Antigua and Barbuda if that person knows or has reason to suspect that they are derived directly or indirectly from any unlawful activity. The MLPA covers institutions defined under the Banking Act, IBCA, and the Financial Institutions (NonBanking) Act, which include offshore banks, IBCs, money service businesses, credit unions, building societies, trust businesses, casinos, Internet gaming companies, and sports betting companies. Intermediaries such as lawyers and accountants are not included in the MLPA. The MLPA requires reporting entities to report suspicious activity suspected to be related to money laundering, whether a transaction was completed or not. There is no reporting threshold imposed on banks and financial institutions. Internet gaming companies, however, are required by the Interactive Gaming and Interactive Wagering Regulations to report to the ONDCP all payouts over U.S. \$25,000.

The Office of National Drug Control and Money Laundering Policy Act, 2003 establishes the ONDCP as the GOAB's FIU. The ONDCP is an independent organization under the Ministry of National Security and is primarily responsible for the enforcement of the MLPA and for directing the GOAB's anti-money laundering efforts in coordination with the FSRC. The ONDCP assumes the role and fulfills the responsibilities of the Supervisory Authority as described in the MLPA, which includes the supervision of all financial institutions with respect to filing suspicious transaction reports (STRs). Additionally, the ONDCP Act authorizes the director to appoint officers to investigate narcotics trafficking, fraud, money laundering, and terrorist financing offenses. Auditors of financial institutions review their compliance program and submit a report to the ONDCP for analysis and recommendations. The ONDCP has no direct access to databases of financial institutions. Domestically, the ONDCP has a memorandum of understanding with the FSRC and is expected to sign another with the ECCB. Other memoranda of understanding have been drafted to cover all aspects of the ONDCP's relationship with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force.

As of October 2007, the ONDCP had received 43 STRs (down from 52 in 2006), 11 of which were investigated. No arrests, prosecutions or convictions were reported by the GOAB in 2006 or 2007, although there were two arrests in 2005. Antigua and Barbuda has yet to prosecute a money laundering case.

Under the MLPA, a person entering or leaving the country is required to report to the ONDCP whether he or she is carrying U.S. \$10,000 or more in cash or currency. In addition, all travelers are required to

fill out a customs declaration form indicating if they are carrying in excess of U.S. \$10,000 in cash or currency. If so, they may be subject to further questioning and possible search of their belongings by Customs officers. The GOAB Customs Department maintains statistics on cross-border cash reports and seizures for failure to report. This information is shared with the ONDCP and the police.

The Misuse of Drugs Act empowers the court to forfeit assets related to drug offenses. The ONDCP is responsible for tracing, seizing and freezing assets related to money laundering. The ONDCP has the ability to direct a financial institution to freeze property up to seven days, while it makes an application for a freeze order. If a charge is not filed or an application for civil forfeiture is not made within 30 days, the freeze order lapses. Convictions for a money laundering offense make it likely that an application for forfeiture will succeed unless the defendant can show that the property was acquired by legal means or the defendant's business was legitimate. Forfeited assets are placed into the Forfeiture Fund and can be used by the ONDCP for any other purpose. Approximately 20 percent of forfeited assets go to the Consolidated Fund at the Treasury.

The GOAB is currently working on asset forfeiture agreements with other jurisdictions. The director of ONDCP, with Cabinet approval, may enter into agreements and arrangements with authorities of a foreign State, which covers matters relating to asset sharing. There are asset sharing agreements with certain countries, while others are negotiated on an ad hoc basis. The ONDCP is presently overseeing the drafting of MOUs with a number of countries in Central America to enhance asset tracing, freezing and seizure. An MOU has recently been concluded with Canada. Regardless of its own civil forfeiture laws, currently the GOAB can only provide forfeiture assistance in criminal forfeiture cases.

In the past few years, the GOAB has frozen approximately U.S. \$6 million in Antigua and Barbuda financial institutions as a result of U.S. requests and has repatriated approximately U.S. \$4 million. The GOAB has frozen, on its own initiative, over U.S. \$90 million believed to be connected to money laundering cases still pending in the United States and other countries. The GOAB reported seizing U.S. \$420,236 in 2006 and U.S. \$14,753 in 2007.

The GOAB enacted the Prevention of Terrorism Act 2001, amended in 2005, to implement the UN conventions on terrorism. The Act empowers the ONDCP to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law covers any finances in any way related to terrorism. The Act also provides the authority for the seizure of property used in the commission of a terrorism act; seizure and restraint of property that has been, is being or may be used to commit a terrorism offence; forfeiture of property on conviction of a terrorism offence; and forfeiture of property owned or controlled by terrorists. The Act requires financial institutions to report every three months on whether or not they are in possession of any property owned or controlled by or on behalf of a terrorist group. In addition, financial institutions must report every transaction that is suspected to be related to the financing of terrorism to the ONDCP. The Attorney General may revoke or deny the registration of a charity or nonprofit organization if it is believed funds from the organization are being used for financing terrorism. The GOAB circulates lists of terrorists and terrorist entities to all financial institutions in Antigua and Barbuda. No known evidence of terrorist financing has been discovered in Antigua and Barbuda to date. The GOAB does not believe indigenous alternative remittance systems exist in country, and has not undertaken any specific initiatives focused on the misuse of charities and nonprofit entities.

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. As a result of such cooperation, both the United States and Canada have shared forfeited assets with the GOAB on several occasions. The amended Banking Act 2004 enables the ECCB to share information directly with foreign regulators if a memorandum of understanding is established. In 1999, a Mutual Legal Assistance Treaty (MLAT) and an extradition treaty with the United States entered into force. An extradition request related to a fraud and money laundering investigation remains pending under the treaty. The GOAB signed a Tax Information

Exchange Agreement with the United States in December 2001 that allows the exchange of tax information between the two nations.

Antigua and Barbuda is a member of the Caribbean Financial Action Task Force (CFATF) and will undergo a mutual evaluation in early 2008. Antigua and Barbuda is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOAB is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism. The ONDCP is a member of the Egmont Group.

The Government of Antigua and Barbuda has taken steps to combat money laundering and terrorist financing by passing relevant legislation that applies to both domestic and offshore financial institutions, and establishing a thorough regulatory regime. However, the GOAB should implement and enforce all provisions of its anti-money laundering and counter-terrorist financing legislation, including the supervision of its offshore sector and gaming industry. Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case and there are few arrests or prosecutions. The GOAB should conduct more thorough investigations that could lead to higher numbers of arrests, prosecutions, and convictions. Law enforcement and customs authorities should be trained to recognize money laundering typologies that fall outside the formal financial sector. The GOAB should continue its international cooperation, particularly with regard to the timely sharing of statistics, information related to offshore institutions, and seized assets.

Argentina

Argentina is neither an important regional financial center nor an offshore financial center. Money laundering related to narcotics trafficking, corruption, contraband, and tax evasion is believed to occur throughout the financial system, in spite of the efforts of the Government of Argentina (GOA) to stop it. The financial sector's continuing recovery from the 2001-02 financial crisis and post-crisis capital controls may have reduced the incidence of money laundering through the banking system. However, transactions conducted through nonbank sectors and professions, such as the insurance industry, financial advisors, accountants, notaries, trusts, and companies, real or shell, remain viable mechanisms to launder illicit funds. Tax evasion is the predicate crime in the majority of Argentine money laundering investigations. Argentina has a long history of capital flight and tax evasion, and Argentines hold billions of dollars offshore, much of it legitimately earned money that was never taxed.

In 2007, the Argentine Congress passed legislation criminalizing terrorism and terrorist financing. Law 26.268, "Illegal Terrorist Associations and Terrorism Financing", entered into effect in mid-July. The law amends the Penal Code and Argentina's anti-money laundering law, Law No. 25.246, to criminalize acts of terrorism and terrorist financing, and establish terrorist financing as a predicate offense for money laundering. Persons convicted of terrorism are subject to a prison sentence of five to 20 years, and those convicted of financing terrorism are subject to a five to 15 year sentence. The new law provides the legal foundation for Argentina's financial intelligence unit (the Unidad de Información Financiera, or UIF), Central Bank, and other regulatory and law enforcement bodies to investigate and prosecute such crimes. The adoption of counter-terrorist financing legislation effectively removes Argentina from the Financial Action Task Force's (FATF) follow-up process, which began in 2004 to address deficiencies in the GOA's anti-money laundering and counter-terrorist financing (AML/CTF) regime. With the passage of Law 26.268, Argentina also joins Chile, Colombia, and Uruguay as the only countries in South America to have criminalized terrorist financing.

On September 11, 2007, President Nestor Kirchner signed into force the National Anti-Money Laundering and Counter-Terrorism Finance Agenda. The overall goal of the National Agenda is to

serve as a roadmap for fine-tuning and implementing existing money laundering and terrorist financing laws and regulations. The Agenda's 20 individual objectives focus on closing legal and regulatory loopholes and improving interagency cooperation. The next challenge is for Argentine law enforcement and regulatory institutions, including the Central Bank and UIF, to implement the National Agenda and aggressively enforce the newly strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes.

Argentina's primary anti-money laundering legislation is Law 25.246 of May 2000. Law 25.246 expands the predicate offenses for money laundering to include all crimes listed in the Penal Code, sets a stricter regulatory framework for the financial sectors, and creates the UIF under the Ministry of Justice and Human Rights. The law requires customer identification, record keeping, and reporting of suspicious transactions by all financial entities and businesses supervised by the Central Bank, the Securities Exchange Commission (Comisión Nacional de Valores, or CNV), and the National Insurance Superintendence (Superintendencia de Seguros de la Nación, or SSN). The law forbids institutions to notify their clients when filing suspicious transaction reports (STRs), and provides a safe harbor from liability for reporting such transactions. Reports that are deemed by the UIF to warrant further investigation are forwarded to the Attorney General's Office.

Law 26.087 of March 2006 amends and modifies Law 25.246 to address many previous deficiencies in Argentina's anti-money laundering regime. It makes substantive improvements to existing law, including lifting bank, stock exchange, and professional secrecy restrictions on filing suspicious activity reports; partially lifting tax secrecy provisions; clarifying which courts can hear requests to lift tax secrecy requests; and requiring court decisions within 30 days. Law 26.087 also lowers the standard of proof required before the UIF can pass cases to prosecutors, and eliminates the so-called "friends and family" exemption contained in Article 277 of the Argentine Criminal Code for cases of money laundering, while narrowing the exemption in cases of concealment. Overall, the law clarifies the relationship, jurisdiction, and responsibilities of the UIF and the Attorney General's Office, and improves information sharing and coordination. The law also reduces restrictions that have prevented the UIF from obtaining information needed for money laundering investigations by granting greater access to STRs filed by banks. However, the law does not lift financial secrecy provisions on records of large cash transactions, which are maintained by banks when customers conduct a cash transaction exceeding 10,000 pesos (approximately U.S. \$3,200).

In September 2006, Congress passed Law 26.119, which amends Law 25.246 to modify the composition of the UIF. The law reorganized the UIF's executive structure, changing it from a five-member directorship with rotating presidency to a structure that has a permanent, politically-appointed president and vice-president. Law 26.119 also established a UIF Board of Advisors, comprised of representatives of key government entities, including the Central Bank, AFIP, the Securities Exchange Commission, the national counternarcotics secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The Board of Advisors' opinions on UIF decisions and actions are nonbinding.

The UIF has issued resolutions widening the range of institutions and businesses required to report suspicious or unusual transactions beyond those identified in Law 25.246. Obligated entities include the tax authority (Administración Federal de Ingresos Públicos, or AFIP), Customs, banks, currency exchange houses, casinos, securities dealers, insurance companies, postal money transmitters, accountants, notaries public, and dealers in art, antiques and precious metals. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. All suspicious or unusual transactions, regardless of the amount, must be reported directly to the UIF. Obligated entities are required to maintain a database of information related to client transactions, including suspicious or unusual transaction reports, for at least five years and must respond to requests from the UIF for further information within 48 hours. As of September 30, 2007, the UIF had received 2851 reports of suspicious or unusual activities since its inception in 2002, forwarded 165 suspected cases of money laundering to prosecutors for review, and assisted prosecutors with 121 cases. There have been only

two money laundering convictions in Argentina since money laundering was first criminalized in 1989, and none since the passage of Law 25.246 in 2000.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 10,000 pesos, and periodically submit the data to the Central Bank. Law 25.246 requires banks to make available to the UIF upon request records of transactions involving the transfer of funds (outgoing or incoming), cash deposits, or currency exchanges that are equal to or greater than 10,000 pesos (approximately U.S. \$3200). The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over U.S. \$10,000 in currency or monetary instruments. These declarations are required by Resolutions 1172/2001 and 1176/2001, which were issued by the Argentine Customs Service in December 2001. In 2003, the Argentine Congress passed Law 22.415/25.821, which would have provided for the immediate fine of 25 percent of the undeclared amount, and for the seizure and forfeiture of the remaining undeclared currency and/or monetary instruments. However, the President vetoed the law because it allegedly conflicted with Argentina's commitments to MERCOSUR (Common Market of the Southern Cone).

Although the GOA has passed a number of new laws in recent years to improve its AML/CTF regime, Law 25.246 still limits the UIF's role to investigating only money laundering arising from seven specific crimes. The law also defines money laundering as an aggravation after the fact of the underlying crime. A person who commits a crime cannot be independently prosecuted for laundering money obtained from the crime; only someone who aids the criminal after the fact in hiding the origins of the money can be guilty of money laundering. Another impediment to Argentina's anti-money laundering regime is that only transactions (or a series of related transactions) exceeding 50,000 pesos (approximately U.S. \$16,000) can constitute money laundering. Transactions below 50,000 pesos can constitute only concealment, a lesser offense.

In 2006 and 2007, the National Coordination Unit in the Ministry of Justice and Human Rights became fully functional, managing the government's AML/CTF efforts and representing Argentina at the FATF and the Financial Action Task Force for South America (GAFISUD). The Attorney General's special investigative unit set up to handle money laundering and terrorism finance cases began operations in 2007. The proposal by the Argentine Banking Superintendence to create a specialized anti-money laundering and counter-terrorism finance examination program is awaiting authorization and is not yet operational.

Argentina's Narcotics Law of 1989 authorizes the seizure of assets and profits, and provides that these or the proceeds of sales will be used in the fight against illegal narcotics trafficking. Law 25.246 provided that proceeds of assets forfeited under this law can also be used to fund the UIF.

Prior to the passage of terrorist financing legislation in June 2007, the Central Bank was the lead Argentine entity responsible for issuing regulations on combating the financing of terrorism. The Central Bank issued Circular A 4273 in 2005 (titled "Norms on 'Prevention of Terrorist Financing'"), requiring banks to report any detected instances of the financing of terrorism. The Central Bank regularly updates and modifies the original Circular. The Central Bank of Argentina also issued Circular B-6986 in 2004, instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. It modified this circular with Resolution 319 in October 2005, which expands Circular B-6986 to require financial institutions to check transactions against the terrorist lists of the United Nations, United States, European Union, Great Britain, and Canada. No assets have been identified or frozen to date. The GOA and Central Bank assert that they remain committed to freezing assets of terrorist groups identified by the United Nations if detected in Argentine financial institutions.

In December 2006, the U.S. Department of Treasury designated nine individuals and two entities that have provided financial or logistical support to Hizballah and operate in the territory of neighboring countries that border Argentina. This region is commonly referred to as the Tri-Border Area, between Argentina, Brazil, and Paraguay. According to the designation, the nine individuals have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hizballah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used in generating or moving terrorist funds. The GOA joined the Brazilian and Paraguayan governments in publicly disagreeing with the designations, stating that the United States had not provided new information proving terrorist financing activity is occurring in the Tri-Border Area.

Working with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina has established a Trade Transparency Unit (TTU). The TTU examines anomalies in trade data that could be indicative of customs fraud and international trade-based money laundering. The TTU has discovered a major discrepancy in import-export data and is supporting an on-going investigation. One key focus of the TTU, as well as of other TTUs in the region, will be financial crimes occurring in the Tri-Border Area. The creation of the TTU was a positive step towards complying with FATF Special Recommendation VI on terrorist financing via alternative remittance systems. Trade-based systems often use fraudulent trade documents and over and under invoicing schemes to provide counter valuation in value transfer (hawala) and settling accounts.

The GOA remains active in multilateral counternarcotics and international AML/CTF organizations. It is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, the FATF and GAFISUD. The GOA is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Argentina participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Tri-Border Area countries. The UIF has been a member of the Egmont Group since July 2003, and has signed memoranda of understanding regarding the exchange of information with a number of other financial intelligence units. The GOA and the USG have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force in 2000.

With passage of counter-terrorist financing legislation and strengthened mechanisms available under Laws 26.119, 26.087, and 25.246, Argentina has the legal and regulatory capability to combat and prevent money laundering and terrorist financing. Furthermore, the new national anti-money laundering and counter-terrorist financing agenda provides the structure for the Government of Argentina to improve existing legislation and regulation, and enhance inter-agency coordination. The challenge now is for Argentine law enforcement and regulatory agencies and institutions, including the Ministry of Justice, Central Bank, and UIF, to implement the National Agenda and aggressively enforce the newly strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes. The GOA could further improve its legal and regulatory structure by enacting legislation to expand the UIF's role to enable it to investigate money laundering arising from all crimes, rather than just seven enumerated crimes; establishing money laundering as an autonomous offense; and eliminating the current monetary threshold of 50,000 pesos (approximately U.S. \$16,000) required to establish a money laundering offense. To comply with the FATF recommendation on the regulation of bulk money transactions, Argentina should review the legislation vetoed in 2003 to find a way to regulate such transactions consistent with its MERCOSUR obligations. Other continuing priorities are the effective sanctioning of officials and institutions that fail to comply with the reporting requirements of the law, the pursuit of a training program for all levels of the criminal justice system, and the provision of the necessary resources to the UIF to carry out its

mission. There is also a need for increased public awareness of the problem of money laundering and its connection to narcotics, corruption, and terrorism.

Aruba

Aruba is an autonomous and largely self-governing Caribbean island under the sovereignty of the Kingdom of the Netherlands; foreign, defense and some judicial functions are handled at the Kingdom level. Due to its geographic location, casinos, and free trade zones, Aruba is both attractive and vulnerable to narcotics trafficking and money laundering.

Aruba has four commercial and two offshore banks, one mortgage bank, one credit union, an investment bank, a finance company, and eleven casinos. The island also has four registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), eight life insurance companies, 13 general insurance companies, four captive insurance companies, and 11 company pension funds. There are approximately 5,343 limited liability companies (NVs), of which 372 are offshore limited liability companies or offshore NVs, which may operate until 2008. In addition, there are approximately 2,763 Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NVs and the AECs are the primary methods used for international tax planning in Aruba. The offshore NVs pay a small percentage tax and are subject to more regulation than the AECs. The AECs pay an annual U.S. \$280 registration fee and must have a minimum of U.S. \$6,000 in authorized capital. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. The AECs must have a local registered agent, which must be a trust company.

In 2001, the Government of Aruba (GOA) made a commitment to the Organization for Economic Cooperation and Development (OECD), in connection with the Harmful Tax Practices initiative, to modernize fiscal legislation in line with OECD standards. In 2003, the GOA introduced a New Fiscal Regime (NFR) containing a dividend tax and imputation payment. As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AECs. Nevertheless, as a result of commitments to the OECD, the regime was brought in line with OECD standards as of January 2006. As a result of the NFR, Aruba's offshore regime will cease operations by July 1, 2008.

Aruba currently has three designated free zones: Oranjestad Free Zone, Bushiri Free Zone, and the Barcadera Free Zone. The free zones are managed and operated by Free Zone Aruba (FZA) NV, a government limited liability company. Originally, only companies involved in trade or light industrial activities, including servicing, repairing and maintenance of goods with a foreign destination, could be licensed to operate within the free zones. However, State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before being admitted to operate in the free zone, companies must submit a business plan along with personal data of managing directors, shareholders, and ultimate beneficiaries, and must establish a limited liability company founded under Aruban law intended exclusively for free zone operations. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones in an effort to control trade-based money laundering. The guidelines were adopted at the CFATF Ministerial Council in October 2001. Free Zone Aruba NV is continuing the process of implementing and auditing the standards that have been developed.

The Central Bank of Aruba is the supervisory and regulatory authority for credit institutions, insurance companies, company pension funds, and money transfer companies. The State Ordinance on the Supervision of Insurance Business (SOSIB) brought all insurance companies under the supervision of the Central Bank. The insurance companies already active before the introduction of this ordinance were also required to obtain a license from the Central Bank. The State Ordinance on the Supervision

of Money-Transfer Companies, effective August 2003, places money transfer companies under the supervision of the Central Bank. Quarterly reporting requirements became effective in 2004. A State Ordinance on the supervision of trust companies, which will designate the Central Bank as the supervisory authority, is currently being drafted.

Aruba's State Ordinance on the penalization money laundering of 1993 (AB 1993 no. 70) was repealed in 2006 through amendments to the Penal Code (AB 2006 no. 11). The GOA's anti-money laundering legislation extends to all crimes, and the Penal Code allows for conviction-based forfeiture of assets. All financial and nonfinancial institutions, which include banks, money remitters, brokers, insurance companies, and casinos, are obligated to identify clients that conduct transactions over 20,000 Aruban guilders (approximately U.S. \$11,300), and report suspicious transactions to Aruba's financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT). Obligated entities are protected from liability for reporting suspicious transactions. The GOA's anti-money laundering requirements do not extend to such nonfinancial businesses and professions as lawyers, accountants, the real estate sector, or dealers in precious metals and jewels.

The MOT was established in 1996. The MOT is authorized to inspect all obligated entities for compliance with reporting requirements for suspicious transactions and the identification requirements for all financial transactions. The MOT is currently staffed by 10 employees. In 2007, the MOT received approximately 5,715 suspicious transaction reports (STRs), resulting in 180 investigations conducted and 47 cases transferred to the appropriate authorities. The MOT reports that very few STRs are filed by the gaming and insurance sectors.

In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the cross-border transportation of currency in excess of 20,000 Aruban guilders to the customs department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review, and in 2007, approximately 820 such reports were submitted.

The MOT shares information with other national government departments. In April 2003, the MOT signed an information exchange agreement with the Aruba Tax Office, which is in effect and being implemented. The MOT and the Central Bank have also signed an information exchange memorandum of understanding (MOU), effective January 2006. The MOT is not linked electronically to the police or prosecutor's office. The MOT is a member of the Egmont Group and is authorized by law to share information with members of the Egmont Group through MOUs.

In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. The GOA has a local committee comprised of officials from different departments of the Aruban Government, under the leadership of the MOT, to oversee the implementation of Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations on terrorist financing. The local committee, FATF Committee Aruba, reviewed the GOA anti-money laundering legislation and proposed, in accordance with the nine FATF Special Recommendations on Terrorist Financing, amendments to existing legislation and introduction of new laws. In 2007, the Parliament of Aruba approved the Ordinance on Sanctions 2006 (AB 2007 no. 24), to enhance the GOA's compliance with the FATF Special Recommendations. The GOA and the Netherlands formed a separate committee in 2004 to ensure cooperation of agencies within the Kingdom of the Netherlands in the fight against cross-border organized crime and international terrorism.

The bilateral agreement between the Netherlands and the United States Government (USG) regarding mutual cooperation in the tracing, freezing, seizure, and forfeiture of proceeds and instrumentalities of crime and the sharing of forfeited assets, which entered into force in 1994, applies to Aruba. The Mutual Legal Assistance Treaty between the Netherlands and the USG also applies to Aruba, though it is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba. The Tax

Information Exchange Agreement with the United States, signed in November 2003, became effective in September 2004.

The Netherlands extended application of the 1988 UN Drug Convention to Aruba in 1999, the UN International Convention for the Suppression of the Financing of Terrorism in 2005, and the UN Convention against Transnational Organized Crime in 2007. The Netherlands has not yet extended application of the UN Convention against Corruption to Aruba. Aruba participates in the FATF and the FATF mutual evaluation program as part of the Kingdom of the Netherlands. The GOA is also a member of CFATF. The MOT became a member of the Egmont Group in 1997. Aruba is also a member of the Offshore Group of Banking Supervisors.

The Government of Aruba has shown a commitment to combating money laundering and terrorist financing by establishing an anti-money laundering and counter-terrorist financing regime that is generally consistent with the recommendations of the FATF and CFATF. Aruba should take additional steps to immobilize bearer shares under its fiscal framework and to enact its long-pending ordinance addressing the supervision of trust companies. The GOA should ensure that all obligated entities are fully complying with their anti-money laundering and counter-terrorist financing reporting requirements, and consider extending these reporting requirements to designated nonfinancial businesses and professions.

Australia

Australia is one of the major centers for capital markets in the Asia-Pacific region. In 2006-07, turnover across Australia's over-the-counter and exchange-traded financial markets was AU \$120 trillion (approximately U.S. \$108 trillion). Australia's total stock market capitalization is over AU \$1.63 trillion (approximately U.S. \$1.5 trillion), making it the eighth largest market in the world, and the third largest in the Asia-Pacific region behind Japan and Hong Kong. Australia's foreign exchange market is ranked seventh in the world by turnover, with the U.S. dollar and the Australian dollar the fourth most actively traded currency pair globally. While narcotics offences provide a substantial source of proceeds of crime, the majority of illegal proceeds are derived from fraud-related offences. A 2004 Australian Government estimate suggests that the amount of money laundered in Australia is in the vicinity of AU \$4.5 billion (approximately U.S. \$4 billion) per year.

The Government of Australia (GOA) has maintained a comprehensive system to detect, prevent, and prosecute money laundering. The last five years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. Australia's system has evolved over time to address new money laundering and terrorist financing risks identified through continuous consultation between government agencies and the private sector.

In March 2005, the Financial Action Task Force (FATF) conducted its on-site Mutual Evaluation (FATFME) of Australia's anti-money laundering/counter-terrorist financing (AML/CTF) system. Australia was one of the first member countries to be evaluated under FATF's revised recommendations. The FATF's findings from the mutual evaluation of Australia were published in October 2005; and Australia was found to be compliant or largely compliant with just over half of the FATF Recommendations. The FATFME noted that although Australia "has a comprehensive money laundering offense . . . the low number of prosecutions . . . indicates . . . that the regime is not being effectively implemented."

In response, the GOA has committed to reforming Australia's AML/CTF system to implement the revised FATF Forty plus Nine recommendations. The Attorney General's Department (AGD) is coordinating this process, now underway, which is significantly reshaping Australia's AML/CTF regime and bringing it into line with current international best practices.

Australia criminalized money laundering related to serious crimes with the enactment of the Proceeds of Crime Act 1987. This legislation also contained provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. It was superseded by two acts that came into force on January 1, 2003 (although proceedings that began prior to that date under the 1987 law will continue under that law). The Proceeds of Crime Act 2002 provides for civil forfeiture of proceeds of crime as well as for continuing and strengthening the existing conviction-based forfeiture scheme that was in the Proceeds of Crime Act 1987. The Proceeds of Crime Act 2002 also enables freezing and confiscation of property used in, intended to be used in, or derived from, terrorism offenses. It is intended to implement obligations under the UN International Convention for the Suppression of the Financing of Terrorism and resolutions of the UN Security Council relevant to the seizure of terrorism-related property. The Act also provides for forfeiture of literary proceeds where these have been derived from commercial exploitation of notoriety gained from committing a criminal offense.

The Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002 (POCA 2002), repealed the money laundering offenses that had previously been in the Proceeds of Crime Act 1987 and replaced them with updated offenses that have been inserted into the Criminal Code. The new offenses in Division 400 of the Criminal Code specifically relate to money laundering and are graded according both to the level of knowledge required of the offender and the value of the property involved in the activity constituting the laundering. As a matter of policy all very serious offenses are now gradually being placed in the Criminal Code. POCA 2002 also enables the prosecutor to apply for the restraint and forfeiture of property from proceeds of crime. POCA 2002 further creates a national confiscated assets account from which, among other things, various law enforcement and crime prevention programs may be funded. Recovered proceeds can be transferred to other governments through equitable sharing arrangements.

The Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act) received Royal Assent on December 12, 2006 and was subsequently amended on April 12, 2007. The Act forms part of a legislative package that implements the first tranche of reforms to Australia's AML/CTF regulatory regime. The AML/CTF Act covers the financial sector, gambling sector, bullion dealers and any other professionals or businesses that provide particular 'designated services'. The Act imposes a number of obligations on entities that provide designated services, including customer due diligence, reporting obligations, record keeping obligations, and the requirement to establish and maintain an AML/CTF program. The AML/CTF Act implements a risk-based approach to regulation and the various obligations under the Act will be implemented over a two-year period (the final components will commence in December 2008). The legislative framework authorizes operational details to be settled in AML/CTF Rules, which will be developed by the Australian Transaction Reports and Analysis Centre (AUSTRAC) in consultation with industry. During 2006-07, AUSTRAC published 16 Rules relating to the AML/CTF Act, all developed in consultation with industry. AUSTRAC has also published a number of guidance notes for entities, including guidance regarding correspondent banking and providers of designated remittance services.

In 2007, the Australian Government began work on a second tranche of AML/CTF reforms, which will extend regulatory obligations to designated services provided by real estate agents, dealers in precious stones and metals, and specified legal, accounting, trust and company services (lawyers and accountants were included in the first tranche, but only where they compete with the financial sector and not for general services). The AGD has actively engaged with a broad cross-section of entities and interest groups regarding the proposed reforms.

The AML/CTF Act will gradually replace the Financial Transaction Reports Act 1988 (FTR Act) which currently operates concurrently to the AML/CTF Act, providing certain AML/CTF obligations until the various provisions of the new act are fully implemented. The FTR Act was enacted to combat tax evasion, money laundering, and serious crimes and it requires banks and nonbanking financial

entities (collectively referred to as cash dealers) to verify the identities of all account holders and signatories to accounts, and to retain the identification record, or a copy of it, for seven years after the day on which the relevant account is closed. A cash dealer, or an officer, employee, or agent of a cash dealer, is protected against any action, suit, or proceeding in relation to the reporting process. The FTR Act also establishes reporting requirements for Australia's cash dealers. Required to be reported are: suspicious transactions, cash transactions equal to or in excess of AU \$10,000 (approximately U.S. \$9,000), and all international funds transfers into or out of Australia, regardless of value. The FTR Act also obliges any person causing an international movement of currency of Australian AU \$10,000 (or a foreign currency equivalent) or more, into or out of Australia, either in person, as a passenger, by post or courier to make a report of that transfer. When the reporting obligations of the AML/CTF Act are implemented in December 2008, reporting entities will be required to report suspicious matters (which is broader than the current obligation to report suspect transactions), international funds transfers, and threshold transactions (more than AU \$10,000), as well as being obliged to report details of their compliance with the AML/CTF legislation in the form of compliance reports.

FTR Act reporting also applies to nonbank financial institutions such as money exchangers, money remitters, stockbrokers, casinos and other gambling institutions, bookmakers, insurance companies, insurance intermediaries, finance companies, finance intermediaries, trustees or managers of unit trusts, issuers, sellers, and redeemers of travelers checks, bullion sellers, and other financial services licensees. Solicitors (lawyers) are also required to report significant cash transactions. Accountants do not have any FTR Act obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

AUSTRAC was established under the FTR Act and is continued in existence by the AML/CTF Act. AUSTRAC is Australia's AML/CTF regulator and specialist financial intelligence unit (FIU). AUSTRAC collects, retains, compiles, analyzes, and disseminates financial transaction report (FTR) information. AUSTRAC also provides advice and assistance to revenue collection, social justice, national security, and law enforcement agencies, and issues guidelines to regulated entities regarding their obligations under the FTR Act, AML/CTF Act and the Regulations and Rules. Under the AML/CTF Act, AUSTRAC now has an expanded role as the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of business sectors. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. During the 2006-07 Australian financial year, AUSTRAC's FTR information was used in 1,529 operational matters. Results from the Australian Taxation Office (ATO) shows that the FTR information contributed to more than AU \$87 million (approximately U.S. \$77 million) in ATO assessments during the year. In 2006-07, AUSTRAC received 15,740,744 financial transaction reports, with 99.7 percent of the reports submitted electronically through the EDDS Web reporting system. AUSTRAC received 24,440 suspect transaction reports (SUSTRs), a decline of 1.5 percent following a 44.1 percent increase in the previous year.

During 2006-07, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 17 percent of the total number of FTRs reported to AUSTRAC in 2006-07 and are reported by cash dealers and solicitors. In 2006-07, AUSTRAC received 2,675,050 SCTRs, an increase of 10.7 percent from the previous year. Cash dealers are also required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 13,017,467 IFTIs to AUSTRAC during the financial year—a 14.0 percent increase from 2005-06. International currency transfer reports (ICTR) are primarily declared to the Australian Customs Service (ACS) by individuals when they enter or depart from Australia. AUSTRAC received 23,351 ICTRs—a 15.9 percent decrease from the previous financial year. The Infringement Notice Scheme (INS) is a new penalty-based scheme introduced in 2007 under the AML/CTF Act to strengthen Australia's cross border movement procedures. An ACS or Australian Federal Police (AFP) officer can issue infringements at the border, where there is a

failure to report a cross border movement of physical currency (CBM-PC) or the cross border movement of a bearer negotiable instrument (CBM-BNI; for example, travelers checks). The issuing of infringements for a failure to report a CBM-BNI is based on disclosure upon request rather than a declaration.

In April 2005, the Minister for Justice and Customs launched AUSTRAC's AML eLearning application. This application has been well received by cash dealers as a tool in providing basic education on the process of money laundering, the financing of terrorism, and the role of AUSTRAC in identifying and assisting investigations of these crimes. In December 2007, the new Minister for Home Affairs launched three new tools to assist industry comply with their AML/CTF obligations, in addition to updating the eLearning application. AUSTRAC Online is a secure Internet-based system which assists entities adhere to their reporting and regulatory obligations, and enables them to access their own information. The AUSTRAC Regulatory Guide is an instructional and 'living' document that assists industry to understand and meet their AML/CTF obligations, which will be updated as further AML/CTF Act provisions are implemented. Lastly, the AUSTRAC Typologies and Case Studies Report 2007 was published to raise industry awareness regarding potential AML/CTF risk factors, methods and typologies.

The Australian Prudential Regulation Authority (APRA) is the prudential supervisor of Australia's financial services sector. AUSTRAC regulates anti-money laundering/counter-terrorist financing (AML/CTF) compliance. The FATFME noted that a comprehensive system for AML/CTF compliance for the entire financial sector needed to be established by the GOA, as does an administrative penalty regime for AML/CTF noncompliance. As a result, the AML/CTF Act has given AUSTRAC a wide range of enhanced enforcement powers to complement the criminal sanctions that were available under the FTR Act. The AML/CTF Act now provides AUSTRAC with a civil penalty framework and other intermediate sanctions, such as enforceable undertakings, remedial directions and external audits for noncompliance. AUSTRAC has conducted very few compliance audits in recent years and places a great deal of emphasis on educating and continuously engaging the private sector regarding the evolution of AML/CTF regime and the attendant reporting requirements. During 2006-07, AUSTRAC conducted 78 educational visits to regulated entities to raise awareness of their obligations under the AML/CTF Act.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002 (SFT Act). The aim of the SFT Act is to restrict the financial resources available to support the activities of terrorist organizations. This legislation criminalizes terrorist financing and substantially increases the penalties that apply when a person uses or deals with suspected terrorist assets that are subject to freezing. The SFT Act enhances the collection and use of financial intelligence by requiring cash dealers to report suspected terrorist financing transactions to AUSTRAC, and relaxes restrictions on information sharing with relevant authorities regarding the aforementioned transactions. The SFT Act also addresses commitments Australia has made with regard to the UNSCR 1373 and is intended to implement the UN International Convention for the Suppression of the Financing of Terrorism. Under this Act three accounts related to an entity listed on the UNSCR 1267 Sanction Committee's consolidated list, the International Sikh Youth Federation, were frozen in September 2002. While there have been some charges laid for acts in preparation of terrorism, there have been no terrorist financing charges or prosecutions under this legislation. The Security Legislation Amendment (Terrorism) Act 2002 also inserted new criminal offenses in the Criminal Code for receiving funds from, or making funds available to, a terrorist organization.

The Anti-Terrorism Act (No.2) 2005 (AT Act), which took effect on December 14, 2006, amends offenses related to the funding of a terrorist organization in the Criminal Code so that they also cover the collection of funds for or on behalf of a terrorist organization. The AT Act also inserts a new offense of financing a terrorist. The AML/CTF Act further addressed terrorist financing by placing an obligation on providers of designated remittance services to register with AUSTRAC.

Investigations of money laundering reside with the AFP and Australian Crime Commission (Australia's only national multi-jurisdictional law enforcement agency). The AFP is the primary law enforcement agency for the investigation of money-laundering and terrorist-financing offences in Australia at the Commonwealth level and has both a dedicated Financial Crimes Unit and well staffed Financial Investigative Teams (FIT) with primary responsibility for asset identification/restraint and forfeiture under the POCA 2002. The Commonwealth Director of Public Prosecutions (CDPP) prosecutes offences against Commonwealth law and to recover proceeds of Commonwealth crime. The main cases prosecuted by the CDPP involve drug importation and money laundering offences. One individual plead guilty to charges of money laundering in 2007, and legal proceedings are underway against a group of individuals arrested in late 2006 for involvement in a multi-million dollar money laundering operation.

In April 2003, the AFP established a Counter Terrorism Division to undertake intelligence-led investigations to prevent and disrupt terrorist acts. A number of Joint Counter Terrorism Teams (JCTT), including investigators and analysts with financial investigation skills and experience, are conducting investigations specifically into suspected terrorist financing in Australia. The AFP also works closely with overseas counterparts in the investigation of terrorist financing, and has worked closely with the FBI on matters relating to terrorist financing structures in South East Asia. In 2006, AFP introduced mandatory consideration of potential money laundering and crime proceeds into its case management processes, thereby ensuring that case officers explore the possibility of money laundering and crime proceeds actions in all investigations conducted by the AFP.

The GOA participates in the Strategic Alliance Group, also known as "5 Eyes". This group of five countries include representatives from the UK Serious Organized Crime Agency (SOCA), the Royal Canadian Mounted Police (RCMP), the Australian Federal Police (AFP), the New Zealand Police (NZP), the United States Immigration and Customs Enforcement (ICE), the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI), all of whom analyze various genres of criminal activity and exchange information and best practices.

Australia is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime and its protocol on migrant smuggling. In September 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. Australia participates actively in a range of international fora, including the FATF, the Pacific Islands Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the Asia/Pacific Group on Money Laundering (APG), of which it serves as permanent co-chair, the GOA has elevated money laundering and terrorist financing issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is an active member of the Egmont Group of Financial Intelligence Units (FIUs). AUSTRAC has signed Exchange Instruments, mostly in the form of Memoranda of Understanding (MOUs) allowing the exchange of financial intelligence, with FinCEN and the FIUs of 48 other countries.

Following the bombings in Bali in October 2002, the Australian Government announced an AU \$10 million (approximately U.S. \$9 million) initiative managed by the Australian Agency for International Development (AusAID), to assist in the development of counterterrorism capabilities in Indonesia. As part of this initiative, the AFP has established a number of training centers such as the Jakarta Centre for Law Enforcement Cooperation. As part of Australia's broader regional assistance initiatives, AUSTRAC continued its South East Asia Counter Terrorism Program of providing capacity building assistance to 10 South East Asian nations, to develop capacity in detecting and dealing with terrorist financing and money laundering. AUSTRAC is also providing further assistance in terms of IT system enhancements to the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center). In the Pacific region, AUSTRAC has developed and provided unique software and training for personnel to six Pacific island FIUs (Cook Islands, Solomon Islands, Samoa, Tonga, Palau and Vanuatu) to fulfill their domestic obligations and share information with foreign analogs. AUSTRAC

is also undertaking IT Needs Assessments in Papua New Guinea and Nauru as part of its engagement with Pacific FIUs. AUSTRAC has worked collaboratively with the Fiji FIU to develop a larger scale information management system solution and enable the collection and analysis of financial transaction reports. The AGD received a grant of AUD7.7 million (approximately U.S. \$6.9 million) over four years to establish the Anti-Money Laundering Assistance Team (AMLAT). AMLAT works cooperatively with the U.S. Department of State-funded Pacific Islands Anti-Money Laundering Program (PALP) to enhance AML/CTF regimes for Pacific island jurisdictions. The PALP, a four-year program, is managed by the Pacific Islands Forum (PIF) and employs residential mentors to develop or enhance existing AML/CTF regimes in the nonFATF member states of the PIF.

The GOA continues to pursue a comprehensive anti-money laundering/counter-terrorist financing regime that meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML/CTF regime, as noted in the FATF mutual evaluation, AUSTRAC has been provided with substantially increased powers to ensure compliance. There will be more on-site compliance audits and AUSTRAC can require regular compliance reports from reporting entities; can initiate monitoring orders and statutory demands for information and documents; can seek civil penalty orders, remedial directions and injunctions; and, can require a reporting entity to subject itself to an external audit of its AML/CTF program. The AML/CTF Act also provides for greater coordination amongst the regulatory agencies of its financial, securities and insurance sectors.

The GOA is continuing its exemplary leadership role in emphasizing money laundering/terrorist finance issues and trends within the Asia/Pacific region and its commitment to providing training and technical assistance to the jurisdictions in that region. Having significantly enhanced its increased focus on AML/CTF deterrence, the Government of Australia should increase its efforts to prosecute and convict money launderers.

Austria

As a major financial center, Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern Europe. According to Austrian National Bank statistics, Austria has one of the highest numbers of banks and bank branches per capita in the world, with about 870 banks and one bank branch for every 1,605 people. Austria is not an offshore jurisdiction. Money laundering occurs within the Austrian banking system as well as in nonbank financial institutions and businesses. The percentage of undetected organized crime may be enormous, with much of it reportedly coming from the former Soviet Union. Money laundered by organized crime groups derives primarily from serious fraud, corruption, narcotics trafficking and trafficking in persons. Criminal groups use various instruments to launder money, including informal money transfer systems, the Internet, and offshore companies.

Austria criminalized money laundering in 1993. Predicate offenses include terrorist financing and other serious crimes. Regulations are stricter for money laundering by criminal organizations and terrorist “groupings,” because in such cases the law requires no proof that the money stems directly or indirectly from prior offenses.

Amendments to the Customs Procedures Act and the Tax Crimes Act of 2004 and 2006 address the problem of cash couriers and international transportation of currency and monetary instruments from illicit sources. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, to implement the European Union (EU) regulation on controls of cash entering or leaving the EU, the Government of Austria (GOA) requires an oral or written declaration for cash amounts of 10,000 euros (approximately U.S. \$13,500) or more. This declaration, which includes information on source and use, must be provided when crossing an external EU border. In December 2007 the new Schengen countries were adopted, making it possible

to travel from Estonia to Portugal without border controls. Spot checks for currency at border crossings and on Austrian territory do occur. Customs officials have the authority to seize suspect cash, and will file a report with the Austrian Financial Intelligence Unit (FIU) in cases of suspected money laundering. Austria has no database for cash smuggling reports.

The Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The law requires financial institutions to identify all customers when beginning an ongoing business relationship. In addition, the Banking Act requires customer identification for all transactions of more than 15,000 euros (U.S. \$20,250) for customers without a permanent business relationship with the bank. Identification procedures require that all customers appear in person and present an official photo identification card. These procedures also apply to trustees of accounts, who must disclose the identity of the account beneficiary. Procedures allow customers to carry out nonface-to-face transactions, including Internet banking, on the basis of a secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

To implement the EU's Third Money Laundering Directive (Directive 2005/60/EC), an amendment to the Banking Act has been in effect since January 1, 2008. The new regulations will tighten customer identification procedures by requiring renewed identification in case of doubt about previously obtained ID documents or data as well as requiring personal appearances of trustees. Regulations will also require institutions to determine the identity of beneficial owners and introduce risk-based customer analysis for all customers. Financial institutions must also begin to implement these requirements in their subsidiaries abroad. The 2008 Banking Act amendment also broadens the reporting requirement by replacing "well-founded suspicion" with "suspicion or probable reason to assume" that a transaction serves the purpose of money laundering or terrorist financing or that a customer has violated his duty to disclose trustee relationships.

Enhanced due diligence obligations will apply if the customer has not been physically present for identification purposes (for example, nonface-to-face transactions, Internet banking), and with regard to cross-border correspondent banking relationships. In cases where a financial institution is unable to establish customer identity or obtain other required information on the business relationship, it must decline to enter into a business relationship or process a transaction, or terminate the business relationship. The institution must also consider reporting the case to the FIU. The law also requires financial institutions to keep records on customers and account owners. The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options, and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act's identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. An amendment to the Insurance Act of 1997, in effect since January 1, 2008, tightened record keeping requirements for insurance companies.

The Banking Act includes a due diligence obligation, and the law holds individual bankers responsible if their institutions launder money. The Banking Act and other laws provide "safe harbor" to obligated reporting individuals, including bankers, auctioneers, real estate agents, lawyers, and notaries. The law excuses those who report from liability for damage claims resulting from delays in completing suspicious transactions. Although there is no requirement for banks to report large currency transactions, unless they are suspicious, the FIU provides outreach and information to banks to raise awareness of large cash transactions.

On January 1, 2008, responsibility for on-site inspections of banks, exchange businesses and money transmitters moved from the Financial Market Authority (FMA) to the Austrian National Bank. These on-site inspections, including inspections at subsidiaries abroad, are all-inclusive, and will require analysis of financial flows and compliance with money laundering regulations. Money remittance

businesses require a banking license from the FMA and are subject to supervision. Informal remittance systems such as hawala exist in Austria, but are subject to administrative fines for carrying out banking business without a license. On its website, the FMA has published several circular letters with details on customer identification, money laundering and terrorist financing regulations, and reporting of suspicious transactions.

The Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals introduce additional money laundering and terrorist financing regulations concerning customer identification, reporting of STRs and record keeping for dealers in high value goods, auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors. To implement the EU's Third Money Laundering Directive, amendments to the Stock Exchange Act, the Securities Supervision Act, the Insurance Act, and Austrian laws governing lawyers and notaries are in effect since January 1, 2008. Amendments to the Gambling Act and the law governing accounting professionals are pending approval. These introduced stricter regulations regarding customer identification procedures, including requiring customer identification for all transactions of more than 15,000 euros (U.S. \$20,250) for customers without a permanent business relationship. Lawyers and notaries are exempt from their reporting obligation for information obtained in course of judicial proceedings or providing legal advice to a client unless the client has sought legal advice for laundering money or financing terrorism. The Business Code amendment will require all traders, not only dealers in high-value goods, auctioneers and real estate agents, to establish the identity of customers for cash transactions of 15,000 euros (U.S. \$20,250) or more.

The EU regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007, and became immediately and directly applicable in Austria. Since November 1, 2007, financial institutions require customer identification for all cash fund transfers of 1,000 euros (U.S. \$1,350) or more.

Austria's financial intelligence unit (FIU) is located within the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). The FIU is the central repository of suspicious transaction reports (STRs) and has police powers. During the first ten months of 2007, the FIU received approximately 830 STRs from banks—a significant increase from the 692 suspicious transactions reported in 2006. The FIU has also responded to requests for information from Interpol, Europol, other FIUs, and other authorities. Although no information for 2007 convictions is currently available, there were three money laundering convictions in 2006.

Since 1996, legislation has provided for asset seizure and the forfeiture of illegal proceeds. The banking sector generally cooperates with law enforcement efforts to trace funds and seize illicit assets. Austria has regulations in the Code of Criminal Procedure that are similar to civil forfeiture in the U.S. In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation. In the first ten months of 2007, Austrian courts froze assets worth more than 100 million euros (U.S. \$135 million).

The Extradition and Judicial Assistance Law provides for expedited extradition; expanded judicial assistance; acceptance of foreign investigative findings in the course of criminal investigations; and enforcement of foreign court decisions. Austria's strict bank secrecy regulations can be lifted in cases of suspected money laundering. Moreover, bank secrecy does not apply in cases in which banks and other financial institutions must report suspected money laundering.

The 2002 Criminal Code Amendment (Federal Law Gazette number I/134 of August 13, 2002) introduced the following criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism, in line with United Nations Security Council Resolution 1373. The Criminal Code defines "financing of terrorism" as a separate criminal offense category, punishable in its own right. Terrorist financing is also included in the list of criminal offenses subject to domestic jurisdiction and punishment, regardless of the laws where the act occurred. The money laundering

offense is also expanded to terrorist “groupings.” The Federal Economic Chamber’s Banking and Insurance Department, in cooperation with all banking and insurance associations, has published an official Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism. The law also gives the judicial system the authority to identify, freeze, and seize terrorist financial assets. Asset forfeiture regulations cover funds collected or held available for terrorist financing, and permit freezing and forfeiture of all assets that are in Austria, regardless of whether the crime was committed in Austria or the whereabouts of the criminal.

The Austrian authorities distribute to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee’s consolidated list, as well as the list of Specially Designated Global Terrorists that the United States has designated pursuant to E.O. 13224, and those distributed by the EU to members. According to the Ministry of Justice and the FIU, no accounts found in Austria have shown any links to terrorist financing. The FIU immediately shares all reports on suspected terrorist financing with the Austrian Interior Ministry’s Federal Agency for State Protection and Counterterrorism (BVT). Figures on suspected terrorist financing transaction reports are not available. There were no convictions for terrorist financing in 2006.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The GOA has implemented the Financial Action Task Force (FATF) Special Recommendation on Terrorist Financing regarding nonprofit organizations. The Law on Associations covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, bylaws, organization, management, association registers, appointment of auditors, and detailed accounting requirements. Since January 1, 2007, associations whose finances exceed a certain threshold are subject to special provisions. Each association must appoint two independent auditors and must inform its members about its finances and the auditor’s report. Associations with a balance sheet exceeding 3 million euros (U.S. \$4.05 million) or annual donations of more than 1 million euros (U.S. \$1.35 million) must appoint independent auditors to review and certify the financial statements. Public collection of donations requires advance permission from the authorities. The Central Register of Associations offers basic information on all registered associations in Austria free of charge via the Internet. Stricter customer identification procedures and due diligence obligations for financial institutions will implement an additional layer to monitor charities and nonprofit organizations, particularly in cases where business relationships suggest that they could be connected to money laundering or terrorist financing.

The Law on Responsibility of Associations maintains criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships and European Economic Interest Groupings, but not charitable or nonprofit entities. The law covers all crimes listed in the Criminal Code, including corruption, money laundering and terrorist financing.

The GOA is generally cooperative with U.S. authorities in money laundering cases. Austria has not enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. However, a bilateral U.S.-Austria agreement on sharing of forfeited assets is pending parliamentary ratification. In addition to the exchange of information with home country supervisors permitted by the EU, Austria has defined this information exchange in agreements with more than a dozen other EU members including the United Kingdom, and with Croatia.

Austria is a party to the 1988 UN Drug Convention, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Austria is a member of the EU and the FATF and will undergo a FATF mutual evaluation in 2008. The FIU is a member of the Egmont Group.

The Government of Austria has implemented a viable comprehensive anti-money laundering and counter-terrorist financing regime. The GOA should ensure that it provides the FIU and law enforcement the resources that they require to effectively perform their functions. The GOA should introduce safe harbor legislation protecting FIU and other government personnel from damage claims as a result of their work. Customs authorities should continue spot-checking operations for bulk cash smuggling despite the lack of border controls with Austria's neighbors. The GOA also should consider enacting legislation that will provide for asset sharing with other governments.

Bahamas

The Commonwealth of The Bahamas is an important regional and offshore financial center. The financial services sector provides a vital economic contribution to The Bahamas, accounting for approximately 15 percent of the country's gross domestic product. The U.S. dollar circulates freely in The Bahamas, and is accepted everywhere on par with the Bahamian dollar. Money laundering in The Bahamas is primarily related to financial fraud and the proceeds of drug trafficking. Illicit proceeds from drug trafficking usually take the form of cash or are quickly converted into cash. The strengthening of anti-money laundering laws has made it increasingly difficult for most drug traffickers to deposit large sums of cash. As a result, drug traffickers store extremely large quantities of cash in security vaults at properties deemed to be safe houses. Other money laundering trends include the purchase of real estate, large vehicles and jewelry, as well as the processing of money through a complex web of legitimate businesses and international business companies.

There are presently four casinos operating in The Bahamas, with three new casinos scheduled to open within the next few years. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten Internet gaming sites based in The Bahamas, although Internet gambling is illegal in The Bahamas. Under Bahamian law, Bahamian residents are prohibited from gambling. The Gaming Board of The Bahamas issues licenses and has anti-money laundering oversight for the gaming industry. Freeport is the only free trade zone in The Bahamas. There are no indications that it is used to launder money.

The financial sector of The Bahamas is comprised of onshore and offshore financial institutions, which include banks and trust companies, insurance companies, securities firms and investment funds administrators, financial and corporate service providers, cooperatives, societies, and designated nonfinancial businesses and professions (including accountants, lawyers, real estate agents, and casinos). The Bahamas has six financial sector regulators: the Central Bank of the Bahamas, which is responsible for licensing and supervision of banks and trust companies; the Securities Commission, responsible for regulating the securities and investment funds industry; the Compliance Commission, which supervises financial sector businesses that are not subject to prudential supervision such as lawyers and accountants; the Inspector of Financial and Corporate Service Providers (IFCSP), which licenses and supervises company incorporation agents and other financial service providers; the Director of Societies, which regulates credit unions and societies; and the Registrar of Insurance Companies. These six regulators comprise the Group of Financial Sector Regulators (GFSR). The GFSR meets on a monthly basis to facilitate information sharing between domestic and foreign regulators and discuss cross-cutting regulatory issues, including anti-money laundering.

The Central Bank Act 2000 (CBA) and The Banks and Trust Companies Regulatory Act 2000 (BTCRA) enhance the supervisory powers of the Central Bank to, among other things, conduct on-site and off-site inspections of banks and enhance cooperation between overseas regulatory authorities and the Central Bank. The BTCRA expands the licensing criteria for banks and trust companies, enhances the supervisory powers of the Inspector of Banks and Trust Companies, and enhances the role of the Central Bank Governor. These expanded rights include the right to deny licenses to banks or trust companies deemed unfit to transact business in The Bahamas. Draft legislation has been prepared to

provide the Central Bank with the mandate to supervise nonbank money transmission businesses. Currently, these institutions are licensed and regulated by the IFCSP, and are supervised by the Compliance Commission for anti-money laundering and counter-terrorist financing purposes.

In 2001, the Central Bank enacted a physical presence requirement that means “managed banks” (those without a physical presence but which are represented by a registered agent such as a lawyer or another bank) must either establish a physical presence in The Bahamas (an office, separate communications links, and a resident director) or cease operations. The transition to full physical presence is complete. Some industry sources have suggested that this requirement has contributed to a decline in banks and trusts from 301 in 2003 to 139 as of June 30, 2007.

The International Business Companies Act 2000 and 2001 (Amendments) enacts provisions that abolish bearer shares, require international business companies (IBCs) to maintain a registered office in The Bahamas, and require the registered office to maintain a copy of the names and addresses of the directors and officers and a copy of the shareholders register. A copy of the register of directors and officers must also be filed with the Registrar General. There are approximately 115,000 registered IBCs, only 42,000 of which are active. Only banks and trust companies licensed under the BTCRA and financial and corporate service providers licensed under the Financial Corporate Service Providers Act (FCSPA) may provide registration, management, administration, registered agents, registered offices, nominee shareholders, and officers and directors for IBCs. As of year-end 2007, there were 139 banks and trust companies in the Bahamas.

The Proceeds of Crime Act 2000 criminalizes money laundering. The Financial Transaction Reporting Act 2000 (FTRA) establishes “know your customer” (KYC) requirements. By December 31, 2001, financial institutions were obliged to verify the identities of all their existing account holders and of customers without an account who conduct transactions over \$10,000. All new accounts established in 2001 or later have to be in compliance with KYC rules before they are opened. As of October 2006, the Central Bank reported full compliance with KYC requirements. All nonverified accounts have been frozen.

The Bahamas Financial Intelligence Unit (FIU), established by the FIU Act 2000, operates as an independent administrative body under the Office of the Attorney General, and is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs). The FTRA requires financial and nonfinancial institutions to report suspicious transactions to the FIU when the institution suspects or has reason to believe that any transaction involves the proceeds of crime. The FIU Act 2000 protects obligated entities from criminal or civil liability for reporting transactions. Financial institutions are required by law to maintain records related to financial transactions for no less than five years. If money laundering is suspected, the FIU will disseminate STRs to the Tracing and Forfeiture/Money Laundering Investigation Section (T&F/MLIS) of the Drug Enforcement Unit (DEU) of the Royal Bahamas Police Force for investigation and prosecution in collaboration with the Office of the Attorney General. The FIU receives approximately 190 STRS annually.

The FIU has the administrative power to issue an injunction to stop anyone from completing a transaction for a period of up to three days upon receipt of an STR. In 2006, there were eight cases of asset restraints as a result of STRs. One led to the issuance of a restraint order by the Supreme Court of The Bahamas, in which approximately \$2 million was restrained.

The FIU is responsible for publishing guidelines to advise entities of their reporting obligations. In March 2007, the FIU revised its guidelines to incorporate terrorist financing reporting requirements. These new guidelines give financial institutions information on requirements that must be met, how to identify suspicious transactions, and how to report these transactions to the FIU. In February 2008, the FIU plans to implement the National Strategy to Prevent Money Laundering. The Strategy arose in response to recommendations from the Financial Action Task Force (FATF) and will provide a means to ensure compliance with international anti-money laundering standards.

Between January 2000 and September 2006, 17 individuals were charged with money laundering by the T&F/MLIS, leading to seven convictions. Seven defendants await trial, while two defendants fled the jurisdiction prior to trial. There are no statistics available on prosecutions or convictions for 2007.

As a matter of law, the Government of the Commonwealth of the Bahamas (GOB) seizes assets derived from international drug trade and money laundering. The banking community has cooperated with these efforts. During 2007, nearly \$8 million in cash and assets were seized or frozen. The seized items are in the custody of the GOB. Some are in the process of confiscation while some remain uncontested. Seized assets may be shared with other jurisdictions on a case-by-case basis.

In 2004, the Anti-Terrorism Act (ATA) was enacted to implement the provisions of the UN International Convention for the Suppression of the Financing of Terrorism. In addition to formally criminalizing terrorism and making it a predicate crime for money laundering, the law provides for the seizure and confiscation of terrorist assets, reporting of suspicious transactions related to terrorist financing, and strengthening of existing mechanisms for international cooperation. In 2006, the FIU received two suspicious transaction reports relating to terrorist financing from financial institutions. The reports were analyzed with one forwarded to the police for further investigation.

The Bahamas is a member of the Offshore Group of Banking Supervisors and the Caribbean Financial Action Task Force (CFATF). The Bahamas underwent a CFATF mutual evaluation in June 2006. The report, which was presented at the November 2007 CFATF plenary, will be finalized by January 2008 and published electronically via CFATF's website.

The Bahamas is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Corruption. The Bahamas has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOB has neither signed nor ratified the UN Convention against Corruption. The FIU has been an active participant within the Egmont Group since becoming a member in 2001, and is currently one of the two regional representatives for the Americas. The Bahamas FIU has the ability to sign memoranda of understanding (MOU) with other counterpart FIUs to exchange information. The Bahamas has a Mutual Legal Assistance Treaty with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. The Attorney General's Office for International Affairs manages requests for mutual legal assistance. The Bahamas has an information exchange agreement with the U.S. Securities and Exchange Commission to ensure that requests can be completed in an efficient and timely manner.

The Government of the Commonwealth of The Bahamas has enacted substantial reforms to reduce its vulnerability to money laundering and terrorist financing. The GOB should continue to enhance its anti-money laundering and counter-terrorist financing regime by implementing the National Strategy on the Prevention of Money Laundering. It should also ensure that there is a registry of the beneficial owners of all entities licensed in its offshore financial center. The Bahamas should also provide adequate resources to its law enforcement, prosecutorial and judicial entities to ensure that investigations and prosecutions are satisfactorily completed and requests for international cooperation are efficiently processed. The GOB should become a party to the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the Inter-American Convention against Terrorism.

Bahrain

Bahrain has one of the most diversified economies in the Gulf Cooperation Council (GCC). In contrast to most of its neighbors, oil accounted for only 21.3 percent of Bahrain's gross domestic product (GDP) in 2006. Bahrain has promoted itself as an international financial center in the Gulf region. It hosts a mix of: 387 diverse financial institutions, including 190 banks, of which 54 are wholesale

banks (formerly referred to as off-shore banks or OBUs); 42 investment banks; and 26 commercial banks, of which 19 are foreign-owned. There are 31 representative offices of international banks. Bahrain has 34 Islamic banks and financial institutions. There are 21 moneychangers and money brokers, and several other investment institutions, including 85 insurance companies. The vast network of Bahrain's banking system, along with its geographical location in the Middle East as a transit point along the Gulf and into Southwest Asia, may attract money laundering activities. It is thought that the greatest risk of money laundering stems from questionable foreign proceeds that transit Bahrain.

In January 2001, the Government of Bahrain (GOB) enacted an anti-money laundering law that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulated punishment of up to seven years in prison, and a fine of up to one million Bahraini dinars (approximately \$2.66 million) for convicted launderers and those aiding or abetting them. If organized criminal affiliation, corruption, or a disguised origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 dinars (approximately \$266,000) and a prison term of not less than five years.

On August 12, 2006, Bahrain passed Law 54/2006, amending the anti-money laundering law. Law 54 criminalizes the undeclared transfer of money across international borders for the purpose of money laundering or in support of terrorism. Anyone convicted under the law of collecting or contributing funds, or otherwise providing financial support to a group or persons who practice terrorist acts, whether inside or outside Bahrain, will be subject to imprisonment for a minimum of ten years in prison up to a maximum of a life sentence. The law also stipulates a fine of between the equivalent of \$26,700 and \$1.34 million. Law 54 also codified a legal basis for a disclosure system for cash couriers, though supporting regulations must still be enacted.

A controversial feature of the new law is a revised definition of terrorism that is based on the Organization of the Islamic Conference definition. Article 2 excludes from the definition of terrorism acts of struggle against invasion or foreign aggression, colonization, or foreign supremacy in the interest of freedom and the nation's liberty.

Under the original anti-money laundering law, the Bahrain Monetary Agency (BMA), principal financial sector regulator and de-facto central bank, issued regulations requiring financial institutions to file suspicious transaction reports (STRs), to maintain records for a period of five years, and to provide ready access for law enforcement officials to account information. The BMA became the Central Bank of Bahrain (CBB) in 2006. Immunity from criminal or civil action is given to those who report suspicious transactions. Even prior to the enactment of the new anti-money laundering law, financial institutions were obligated to report suspicious transactions greater than 6,000 dinars (approximately \$15,000) to the BMA/CBB. The current requirement for filing STRs stipulates no minimum thresholds and since 2005 the BMA/CBB has had a secure online website that banks and other financial institutions can use to file STRs.

In September 2006, Law 64/2006 replaced the BMA, which had acted as the de-facto central bank, with the CBB. Law 64 consolidated several laws that had previously governed the various segments of the financial services industry. Under the law, the CBB enjoys reinforced operational independence and enhanced enforcement powers. Part 9 of the law, for example, outlines investigational and administrative proceedings at the CBB's disposal to ensure licensee compliance with rules and regulations. The CBB's compliance arm was upgraded from a unit to a directorate.

The original law also provided for the formation of an interagency committee to oversee Bahrain's anti-money laundering regime. Accordingly, in June 2001, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing was established and assigned the responsibility for developing anti-money laundering policies and guidelines. In early 2006, the chairmanship of the Policy Committee was transferred from the Ministry of Finance to the CBB. The committee's membership was also expanded, to comprise representatives from the Ministries of

Finance, Industry and Commerce, Interior, and Social Development; the Directorates of Customs and Legal Affairs; the Office of Public Prosecution; the National Security Agency; the Bahrain Stock Exchange; and the Central Bank of Bahrain.

In addition, the original law provided for the creation of the Anti-Money Laundering Unit (AMLU) as Bahrain's financial intelligence unit (FIU). The AMLU, which is housed in the Ministry of Interior, is empowered to receive reports of money laundering offenses; conduct investigations; implement procedures relating to international cooperation under the provisions of the law; and execute decisions, orders, and decrees issued by the competent courts in offenses related to money laundering. The AMLU became a member of the Egmont Group of FIUs in July 2003.

The AMLU receives STRs from banks and other financial institutions, investment houses, broker/dealers, moneychangers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions must also file STRs with the Central Bank, which supervises these institutions. Nonfinancial institutions are required under a Ministry of Industry and Commerce (MOIC) directive to also file STRs with that ministry. The Central Bank analyzes the STRs, of which it receives copies, as part of its scrutiny of compliance by financial institutions with anti-money laundering and counter terrorist financing (AML/CTF) regulations, but it does not independently investigate the STRs (responsibility for investigation rests with the AMLU). The Central Bank may assist the AMLU with its investigations where special banking expertise is required.

The Central Bank of Bahrain is the regulator for other nonbanking financial institutions including insurance companies, exchange houses, and capital markets. The Central Bank inspected seven insurance companies in 2006 and had conducted eight more inspections by September 2007. Additional insurance industry inspections are scheduled for 2008. Anti-money laundering regulations for investment firms and securities brokers were revised in April 2006.

In November 2007, the MOIC published new anti-money laundering guidelines, which govern designated nonfinancial businesses and professions (DNFBPs). The MOIC has also announced an increased focus on enforcement, noting some 300 visits to DNFBPs in 2005, including car dealers, jewelers, and real estate agencies. By November 2006, the MOIC had conducted an additional 274 enforcement follow-up visits. A total of 140 of these have been assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from four to seven.

The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the Central Bank's system. Good cooperation exists between MOIC, Central Bank, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU and Central Bank's compliance staff analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that must conduct the actual investigation and forward cases of money laundering and terrorist financing to the Office of the Public Prosecutor.

From January through December 2007, the AMLU has received and investigated 183 STRs, 39 of which have been forwarded to the courts for prosecution. The GOB completed its first successful money laundering prosecution in May 2006. The prosecutions resulted in the convictions of two expatriot felons with sentences of one and three years and fines of \$380 and \$1900 respectively.

In August of 2006, Bahrain passed its first law specifically criminalizing terrorism and establishing harsh penalties for terrorist crimes including financing and money laundering in support of terrorism. The government used this law to bring charges against five suspects in October 2007. The five face a range of charges, including the financing of terrorism. As of January 2008, trial proceedings remained ongoing.

Bahrain is moving ahead with plans to establish a special court to try financial crimes, and judges are undergoing special training to handle such crimes. Six Bahraini judges will join a group of twelve

Jordanian judges on loan to the Ministry of Justice to serve on the court, which is expected to begin hearing cases in March 2008.

There are 54 Central Bank-licensed wholesale banks (formerly referred to as offshore banking units OBUs) that are branches of international commercial banks. The license that changed OBUs to wholesale banks allows wholesale banks to accept deposits from citizens and residents of Bahrain, and undertake transactions in Bahraini dinars (with certain exemptions, such as dealings with other banks and government agencies). In all other respects, wholesale banks are regulated and supervised in the same way as the domestic banking sector. They are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations.

However, Bahrain's Commercial Companies Law (Legislative Decree 21 of 2001) does not permit the registration of offshore companies or international business companies (IBCs). All companies must be resident and maintain their headquarters and operations in Bahrain. Capital requirements vary, depending on the legal form of company, but in all cases the amount of capital required must be sufficient for the nature of the activity to be undertaken. In the case of financial services companies licensed by the Central Bank, various minimum and risk-based capital requirements are also applied in line with international standards of Basel Committee's "Core Principles for Effective Banking Supervision."

BMA Circular BC/1/2002 states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system. In addition, all Central Bank licensees are required to include details of the originator's information with all outbound transfers. With respect to incoming transfers, licensees are required to maintain records of all originator information and to carefully scrutinize inward transfers that do not contain the originator's information, as they are presumed to be suspicious transactions. Licensees that suspect, or have reasonable grounds to suspect, that funds are linked or related to suspicious activities-including terrorist financing-are required to file STRs. Licensees must maintain records of the identity of their customers in accordance with the Central Bank's anti-money laundering regulations, as well as the exact amount of transfers. During 2004, the BMA consulted with the industry on changes to its existing AML/CTF regulations, to reflect revisions by the FATF to its Forty plus Nine Recommendations. Revised and updated BMA regulations were issued in mid-2005.

Legislative Decree No. 21 of 1989 governs the licensing of nonprofit organizations. The Ministry of Social Development (MSD) is responsible for licensing and supervising charitable organizations in Bahrain. In February 2004, as part of its efforts to strengthen the regulatory environment and fight potential terrorist financing, MSD issued a Ministerial Order regulating the collection of donated funds through charities and their eventual distribution, to help confirm the charities' humanitarian objectives. The regulations are aimed at tracking money that is entering and leaving the country. These regulations require organizations to keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are also required to deposit their funds with banks located in Bahrain and may have only one account in one bank. Banks must report to the Central Bank any transaction by a charitable institution that exceeds 3,000 Bahraini dinars (approximately \$8,000). MSD has the right to inspect records of the societies to insure their compliance with the law. The Directorate of Development and Local Societies (DDLs) has a very small staff to undertake the necessary reviews of the financial information submitted by societies or to undertake inspections of these organizations.

Bahrain is a leading Islamic finance center in the region. The sector has grown considerably since the licensing of the first Islamic bank in 1979. Bahrain has 34 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, the Central Bank has developed an appropriate framework for regulating and supervising the Islamic banking sector, applying regulations and supervision as it does with respect to conventional banks. In March 2002, the

Central Bank introduced a comprehensive set of regulations for Islamic banks called the Prudential Information and Regulatory Framework for Islamic Banks (PIRI). The framework was designed to monitor certain banking aspects, such as capital requirements, governance, control systems, and regulatory reporting.

Bahrain is a party to the 1988 UN Drug Convention. Bahrain has signed but not yet ratified the UN Convention against Corruption. In March 2004, Bahrain issued a Legislative Decree ratifying the UN Convention against Transnational Organized Crime. In June 2004, Bahrain published two Legislative Decrees ratifying the UN International Convention for the Suppression of the Financing of Terrorism, and the UN International Convention for the Suppression of Terrorist Bombings. In January 2002, the BMA issued a circular implementing the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing as part of the Central Bank's AML regulations, and subsequently froze two accounts designated by the UNSCR 1267 Sanctions Committee and one account listed under U.S. Executive Order 13224.

In November 2004, Bahrain hosted the inaugural meeting of the Middle East and North Africa Financial Action Task Force (MENAFATF), which decided to place its Secretariat in Bahrain's capital city of Manama. An initial planning meeting was held in Manama in January 2004, and the FATF unanimously endorsed the MENAFATF proposal in July 2004. As a FATF-style regional body, it promotes best practices on AML/CTF issues, conducts mutual evaluations of its members against the FATF standards, and works with its members to comply with international standards and measures. In November 2006, MENAFATF approved a mutual evaluation report on Bahrain. The creation of the MENAFATF is critical to encourage jurisdictions in the region to improve the transparency and regulatory frameworks of their financial sectors.

The Government of Bahrain has demonstrated a commitment to establish a strong anti-money laundering and terrorist financing system and appears determined to engage its large financial sector in this effort. MENAFATF commended Bahrain for its achievements in the area of AML/CTF and praised the government for its commitment to implement the FATF recommendations. However, work remains to be done. Bahrain should continue to develop a disclosure or declaration system for the country's borders that fulfills FATF's Special Recommendation Nine covering bulk cash smuggling. The Anti-Money Laundering Unit should maintain its efforts to obtain and solidify the necessary expertise in tracking suspicious transactions. Nevertheless, there should not be an over-reliance on suspicious transaction reporting to initiate money laundering investigations. Authorities should continue to raise awareness within the capital markets and designated nonfinancial businesses and professions regarding STR reporting obligations and consider applying sanctions for willful noncompliance. Adequate resources should be devoted to the Ministry of Social Development to increase its oversight of NGOs and charities.

Bangladesh

Bangladesh is not a regional or offshore financial center. Under the new caretaker government that declared a state of emergency when it came to power on January 11, 2007, evidence of funds laundered through the official banking system escalated. The new government instituted a stringent anticorruption campaign that netted more than \$30 million in proceeds—a fraction of the estimated total amount of corrupt funds located both domestically and abroad. Money transfers outside the formal banking and foreign exchange licensing system are illegal and therefore not regulated. The principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer money and value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from expatriate Bangladeshi workers.

The Central Bank (CB) reports a considerable increase in remittances since 2002 through official channels. The figure more than doubled from \$2 billion to \$4.3 billion in fiscal year 2006 (July 1-June

30) and then rose again to \$5.9 billion in fiscal year 2007. The increase is due to competition from commercial banks through improved delivery time, guarantees, and value-added services such as group life insurance. However, hundi remains entrenched because it is used to avoid taxes, customs duties, and currency controls. The nonconvertibility of the local currency (the taka) coupled with intense scrutiny on foreign currency transactions in formal financial institutions also contribute to the popularity of both hundi and black market money exchanges.

In Bangladesh, hundi primarily uses trade goods to provide counter valuation or a method of balancing the books in transactions. It is part of trade-based money laundering and a compensation mechanism for the significant amount of goods smuggled into Bangladesh. An estimated \$1 billion dollars worth of dutiable goods are smuggled every year from India into Bangladesh. A comparatively small amount of goods are smuggled out of the country into India. Hard currency and other assets flow out of Bangladesh to support the smuggling networks.

Fighting corruption is a keystone of the caretaker government under the state of emergency. For the past twenty years, corrupt practices became so common that between 2001 and 2005, Bangladesh was ranked by Transparency International's Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2007, Bangladesh was ranked 162 out of 179 countries surveyed. The sweep of corrupt officials and businessmen resulted in over 200 arrests including the two former prime ministers.

Bangladeshis are not allowed to carry cash outside of the country in excess of the equivalent of \$3,000 to South Asian Association for Regional Cooperation (SAARC) countries and the equivalent of \$5,000 to other countries. Proper documents are required by authorized foreign exchange banks and dealers. There is no limit on how much currency can be brought into the country, but amounts over \$5,000 must be declared within 30 days. Customs is primarily a revenue collection agency, accounting for 40-50 percent of Bangladesh's annual government income.

The CB conducts training for commercial banks' headquarters around the country in "know your customer" procedures. Additional training is conducted in identifying suspicious transactions and reporting them to the Central Bank, where the country's financial intelligence unit is located. Since Bangladesh only began in mid-2007 to develop a national identity card (in the form of a voter registration card) and because the vast majority of Bangladeshis do not have a passport, there are difficulties in enforcing customer identification requirements. In most cases, banking records are maintained manually. Some accounting procedures used by the Central Bank do not always achieve international standards. In 2004, the Central Bank issued "Guidance Notes on Prevention of Money Laundering" and designated anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the CB. Banks are required to have an anti-money laundering compliance unit in their head office and a designated anti-money laundering compliance officer in each bank branch. The CB conducts regular training programs for compliance officers based on the Guidance Notes and routinely works with the banks and, if need be, investigates compliance with regulations to curb financial irregularities. Instructors from the CB also conduct regional workshops.

In May 2007 the Central Bank's Anti-Money Laundering Unit (AMLU) was named Bangladesh's Financial Intelligence Unit (FIU). The FIU along with the National Board of Revenue (NBR), the country's tax authority, are the only entities authorized to collect bank statements. While the NBR can freeze an account without a court order, the FIU cannot. Both institutions require a court order to seize and/or forfeit the accounts. The CB has link analysis capability for investigating suspicious transactions.

Since the Money Laundering Prevention Act (MLPA) was enacted in 2002, the Central Bank has received approximately 470 suspicious transaction reports. To date, there have been no successful prosecutions. In part, this is due to procedural problems in adjusting to inter-agency cooperation. A major setback occurred in December 2005 when the newly created Anti-Corruption Commission

(ACC) advised the bank that it would not investigate the cases and returned them. As a result, the Criminal Investigation Division of the national police force agreed to take the cases. During 2006, the bank and police hammered out a procedure to pursue investigations initiated through suspicious transactions reports. With the State of Emergency, a differently configured law enforcement regime headed by military officers began. The results have yielded solid evidence of money laundering. They are not prosecuting these cases as money laundering but as tax evasion or unexplained wealth.

The caretaker Government has pledged to pass amendments to strengthen the current MLPA. The legislation is in the final stages of review. Reportedly, the draft anti-money laundering provisions meet most of the international recommendations set forth by the Egmont Group, including sharing appropriate information with domestic and international law enforcement. The draft legislation addresses asset forfeiture. It does not criminalize terrorist financing. In 2006, the government announced that it wanted a separate Anti-Terrorism law that would criminalize terrorist financing, stipulating that the Anti-Terrorism Act (ATA) would have to be passed before the anti-money laundering legislation. As of late 2007 the anti-terrorism law is still pending with the Law Advisor (de facto Law Minister) repeatedly saying that Bangladesh does not need an anti-terrorism law.

Since 2003, Bangladesh has frozen nominal sums in accounts of three designated entities on the UNSCR 1267 Sanctions Committee's consolidated list. In 2004, following investigation of the accounts of an entity listed on the UNSCR 1267 consolidated list, the Central Bank fined two local banks for failure to comply with CB regulatory directives. In 2005, the Government of Bangladesh (GOB) became a party to the UN International Convention for the Suppression of the Financing of Terrorism and is now a party to twelve UN Conventions and protocols on Terrorism. The GOB is a party to the 1988 UN Drug Convention and the UN Convention against Corruption. The GOB is not a party to the Convention against Transnational Organized Crime. Bangladesh is a member of the Asia-Pacific Group, a Financial Action Task Force (FATF)-style regional body.

Although progress has been made, the Government of Bangladesh should continue to strengthen its anti-money laundering/terrorist finance regime so that it adheres to world standards. Bangladesh should criminalize terrorist finance. There should be technology enhancements to reporting channels from outlying districts to the Central Bank. Bangladesh law enforcement and customs should examine forms of trade-based money laundering. A crackdown on pervasive customs fraud would add new revenue streams for the GOB. Continued efforts should be made to fight corruption, which is intertwined with money laundering, smuggling, customs fraud, and tax evasion. The GOB should ratify the UN Convention against Transnational Organized Crime.

Barbados

A transit country for illicit narcotics, Barbados remains vulnerable to money laundering, which primarily occurs in the formal banking system. Domestically, money laundering is largely drug-related and is appears to be derived from the trafficking of cocaine and marijuana. There is also evidence of Barbados being exploited in the layering stage of money laundering with funds originating abroad. The major source of these funds appears to be connected to fraud.

As of December 2007, there are six commercial banks in Barbados. The offshore sector includes 4,635 international business companies (IBCs), 164 exempt insurance companies and 55 qualified exempt insurance companies, seven mutual funds companies and one exempt mutual fund company, seven trust companies, seven finance companies, and 55 offshore banks. There are no free trade zones and no offshore casinos.

The International Business Companies Act (1992) provides for the general administration of IBCs. The Ministry of Industry and International Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. The International Business (Miscellaneous Provisions)

Act 2001 enhanced due diligence requirements for IBC license applications and renewals. Bearer shares are not permitted, and financial statements of IBCs are audited if total assets exceed \$500,000.

The Central Bank regulates and supervises domestic and offshore banks, trust companies, and finance companies. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The International Financial Services Act (IFSA) requires offshore applicants to disclose directors and shareholders names and addresses. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. The Central Bank has the mandate to conduct on-site examinations of offshore banks. This allows the Central Bank to augment its off-site surveillance system of reviewing anti-money laundering policy documents and analyzing prudential returns. Additionally, permission must be obtained from the Central Bank to move currency abroad.

In 2007, the Central Bank revised the anti-money laundering guidelines for licensed financial institutions to reflect changes in international standards, and to include guidance on how licensees can fulfill their obligations in relation to combating the financing of terrorism. The guideline applies to all entities that are incorporated in Barbados and are licensed under the Financial Institutions Act (FIA) 1996 and the IFSA. The Central Bank conducts off-site surveillance and undertakes regular on-site examinations of licensees to assess compliance with anti-money laundering legislation and regulations. Licenses can be revoked by the Minister of Finance for noncompliance.

The Government of Barbados (GOB) criminalized drug money laundering through the Proceeds of Crime Act and the Drug Abuse (Prevention and Control) Act, 1990-14. The Money Laundering (Prevention and Control) Act 1998 (MLPCA) and subsequent amendments extends the offense of money laundering beyond drug-related crimes by criminalizing the laundering of proceeds from unlawful activities. Under the MLPCA, money laundering is punishable by a maximum of 25 years in prison and a maximum fine of \$1 million. The MLPCA applies to a wide range of financial institutions, including domestic and offshore banks, IBCs, insurance companies, money remitters, investment services, and any other services of a financial nature. These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, report and maintain records of all transactions exceeding \$5,000 for a period of five years, and establish internal audit and compliance procedures. Financial institutions must also report suspicious transactions to the Anti-Money Laundering Authority (AMLA).

Established by the MLPCA, the AMLA supervises financial institutions' compliance with the MLPCA, and issues training requirements and regulations for financial institutions. The AMLA is comprised of nine members including a chairperson, selected from the private sector; a deputy chairperson, from the University of the West Indies; the Solicitor General; the Commissioner of Police; the Commissioner of Inland Revenue; Comptroller of Customs; the Supervisor of Insurance; the Registrar of Corporate Affairs; and a representative of the Central Bank. The Barbados Financial Intelligence Unit (FIU) is the operational arm of the AMLA and carries out the AMLA's supervisory function over financial institutions.

Established in 2000, the FIU is an independent agency housed in the office of the Attorney General. The FIU is responsible for receiving and analyzing suspicious transactions reports from financial institutions; instructing financial institutions to take steps that would facilitate an investigation; and conduct awareness training in regards to record and reporting obligations. There are no laws that prevent disclosure of information to relevant authorities and persons who report to the FIU are protected under the law.

Financial institutions are required to report transactions when the entity has reasonable grounds to suspect the transaction involves the proceeds of crime; involves the financing of terrorism; or is suspicious in nature. In cases where the FIU suspects a transaction involves the proceeds of crime, the FIU will forward the report for further investigation to the Commissioner of Police. As of June 30,

2007, the FIU had received 56 SARs; none were referred to the Commissioner of Police. Government entities and financial institutions are required to provide the FIU with information requested by the Director of FIU. The Royal Barbados Police force pursues all potential prosecutions.

The MLPCA provides only for criminal asset seizure and forfeiture. In 2001, the GOB amended legislation to shift the burden of proof to the accused to demonstrate that property in his or her possession or control is derived from a legitimate source. Absent such proof, the presumption is that such property was derived from the proceeds of crime. The law also enhances the GOB's ability to freeze bank accounts and to prohibit transactions from suspect accounts. Legitimate businesses and other financial institutions are subject to criminal sanction, which can result in the termination of operating licenses. Tracing, seizing and freezing assets may be done by the FIU and the police. Freezing orders are usually granted for six months at a time after which they need to be reviewed. Frozen assets may be confiscated on application by the Director of Public Prosecutions and are paid into the National Consolidated Fund. No asset sharing law has been enacted, but bilateral treaties as well as the Mutual Assistance in Criminal Matters Act have provisions for asset tracing, freezing and seizure between countries.

The Anti-Terrorism Act of 2002 as well as provisions of the Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA) criminalizes the financing of terrorism. The MLFTA is also designed to control bulk cash smuggling and the use of cash couriers. The GOB circulates the names of suspected terrorists and terrorist organizations listed on the United Nations 1267 Sanctions Committee's Consolidated List and the list of Specially Designated Global Terrorists designated by the United States. In 2007, the GOB found no evidence of terrorist financing. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with the United Kingdom, Canada, Finland, Norway, Sweden, Switzerland, and the United States. The United States and the GOB ratified amendments to its bilateral tax treaty in 2004. The treaty with Canada currently allows IBCs and offshore banking profits to be repatriated to Canada tax-free after paying a much lower tax in Barbados. A Mutual Legal Assistance Treaty (MLAT) and an extradition treaty between the United States and the GOB each entered into force in 2000.

Barbados is a member of the Caribbean Financial Action Task Force (CFATF) and underwent a mutual evaluation in December 2006. The report is anticipated to be finalized in the summer of 2008 and published electronically via CFATF's website. Barbados is a member of the Offshore Group of Banking Supervisors, the Caribbean Regional Compliance Association, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU is a member of the Egmont Group. Barbados is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOB has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism.

The Government of Barbados has taken a number of steps in recent years to strengthen its anti-money laundering and counter-terrorist financing legislation, and should continue to implement these reforms. The GOB should be more aggressive in conducting examinations of the financial sector and maintaining strict control over vetting and licensing of offshore entities. The GOB should consider adopting civil forfeiture and asset sharing legislation. The GOB should ensure adequate supervision of nonprofit organizations and charities. It should also work to improve information sharing between regulatory and enforcement agencies. Additionally, Barbados should continue to provide adequate resources to its law enforcement and prosecutorial personnel, to ensure mutual legal assistance treaty

requests are efficiently processed. The GOB should also ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Belarus

Belarus is not a regional financial center. A general lack of transparency throughout the financial sector means that assessing the level of or potential for money laundering and other financial crimes is difficult. Due to excessively high taxes, underground markets, and the dollarization of the economy, a significant volume of foreign-currency cash transactions eludes the banking system. Shadow incomes from offshore companies, filtered through small local businesses, constitute a significant portion of foreign investment. Smuggling is prevalent. Corruption is a severe problem in Belarus, which hinders law enforcement and impedes much-needed reforms. Economic decision-making in Belarus is highly concentrated within the top levels of government. Recent decrees have further concentrated economic power into the hands of the president, granting the Presidential Administration the power to manage, dispose of, and privatize all state-owned property and to confiscate at will any plot of land for agricultural, environmental, recreational, historical, or cultural uses.

Belarus is not considered an offshore financial center, and offshore banks, shell companies, and trusts are not permitted. As of early September 2007, the Belarusian banking sector totaled 27 banks and 383 subsidiaries. Twenty-three banks involved foreign capital, with seven being foreign-owned. In Belarus, there are currently eight offices of foreign banks, including those based in Germany, Latvia, Lithuania, Russia and Ukraine, and a representative office of the CIS Interstate Bank. The state-owned Belarus Bank is the largest and most influential bank in Belarus. In February 2006, the government abolished the 1997 identification requirements for all foreign currency exchange transactions at banks.

Belarus has established six free economic zones (FEZs) based on a 1996 Presidential Decree, one in each of the regions of Belarus. The president creates FEZs upon the recommendation of the Council of Ministers and can dissolve or extend the existence of a FEZ at will. The Presidential Administration, the State Control Committee (SCC), and regional authorities supervise the activities of companies in the FEZs. According to the SCC, applying organizations are fully vetted before they are allowed to operate in an FEZ in an effort to prevent money laundering and terrorism finance. Presidential Decree 66 has tightened FEZ regulations on transaction reporting and security, including mandatory installation of video surveillance systems. A 2005 National Bank resolution changed the status of banks in the zones by removing special provisions. Banks in the zones are currently subject to all regulations that apply to banks outside the zones.

Belarus uses customs declaration forms at points of entry and exit to fulfill cross-border currency reporting requirements for both inbound and outbound currency. Upon entry into or departure from the country, travelers must declare in writing any sum over \$3,000. Travelers crossing the Belarus border with sums exceeding \$10,000 require permission from the National Bank to carry that amount of currency. Officials have reported several cases of attempts to smuggle undeclared cash across borders.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law), amended in 2005, establishes the legal and organizational framework to prevent money laundering and terrorist financing. Measures in the law apply to all entities that conduct financial transactions in Belarus, including credit and financial institutions; stock and currency exchanges; investment funds and dealers in securities; insurance institutions; dealers' and brokers' offices; notary offices; gaming establishments; pawn shops; leasing and estate agents; post offices; dealers in precious stones and metals; attorneys conducting financial transactions on behalf of clients; and other organizations conducting financial transactions.

The AML Law makes individuals, businesses, government entities, and entities without legal status criminally liable for money laundering, although the punishments for laundering or financing

terrorism are not explicitly codified. However, Article 235 of the Belarusian criminal code (“legalization of illegally acquired proceeds”) stipulates penalties of fines or prison terms of up to ten years for money laundering. The law defines “illegally acquired proceeds” as currency, securities or other assets, including real and intellectual property rights, obtained in violation of the law. The National Bank of the Republic of Belarus (National Bank or NBRB) has suggested anti-money laundering and counter-terrorist financing (AML/CTF) regulations, including know your customer (KYC) and due diligence requirements. Although not legally binding, they are treated as mandatory by the institutions that the National Bank supervises. A 2005 International Monetary Fund (IMF) Financial System Stability Assessment pointed out that these regulations needed to be significantly upgraded to meet Financial Action Task Force (FATF) standards.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (Department of Financial Monitoring, or DFM); the Securities Committee; the Ministry of Finance; the Ministry of Justice; the Ministry of Communications and Information; the Ministry of Sports and Tourism; the Committee on Land Resources; the Ministry on Taxes and Duties (MTD); and other state bodies. The MTD also provides oversight and has released binding regulations on its subject institutions.

There is a threshold reporting requirement. Individual and corporate financial transactions exceeding approximately \$27,000 and \$270,000, respectively, are subject to special inspection. Banks that violate the law face fines of up to one percent of their registered capital and suspension of their licenses for up to one year. However, the AML Law exempts most government transactions and those sanctioned by the President from extraordinary inspection. The government has used the AML Law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

In January 2005, the President signed a decree on the regulation of the gaming sector, imposing stricter tax regulations on owners of gaming businesses. In addition, a provision intended to combat money laundering requires those participating in gaming activities to produce identification to receive winnings.

The National Bank is the monitoring agency for the majority of transactions conducted by financial institutions. Information regarding suspicious transactions is reported to the Bank’s Department of Bank Monitoring. Failure to report and transmit required information on financial transactions may subject financial institutions to criminal liability. Although the banking code stipulates that the National Bank has primary regulatory authority over the banking sector, in practice, the Presidential Administration exerts significant influence over it. Any member of the Board of the National Bank may be removed from office by the president with a simple notification to the National Assembly.

Financial institutions conducting transfers subject to special monitoring are required to disclose to the Department of Financial Monitoring (DFM) within one business day the identity of the individuals and businesses ordering the transaction or the person on whose behalf the transaction is being placed, information about the beneficiary of a transaction, and account information and document details used in the transaction. Article 121 of the Banking Code provides a “safe harbor” for banks and other financial institutions that provide otherwise confidential transaction data to investigating authorities, provided the information is given in accordance with the procedures established by law, and reporting individuals are protected by law when notifying authorities of suspicious transactions. Under the State Control Committee (SCC), the Department of Financial Investigations, in conjunction with the Prosecutor General’s Office, has the legal authority to investigate suspicious financial transactions and examine the internal rules and enforcement mechanisms of any financial institution. The DFM also has the authority to initiate its own investigations.

In 2003, Belarus established the Department of Financial Monitoring (DFM) as its financial intelligence unit (FIU). As the primary government agency responsible for gathering, monitoring and disseminating financial intelligence, the DFM analyzes financial information for evidence of money

laundering and forwards it to law enforcement officials for prosecution. The DFM also has the power to penalize those who violate money laundering laws and suspend the financial operations of any company suspected of money laundering or financing terrorism. The DFM cooperates with counterparts in foreign states and with international organizations to combat money laundering and is a member of the Egmont Group. Since its accession to the Egmont Group, the DFM's workload has increased, which the DFM attributes not only to its Egmont membership, but also to increased interest by law enforcement in the FIU's work.

Financial institutions are obligated to report to the DFM transactions subject to special monitoring, including: transactions whose suspected purpose is money laundering or terrorist financing; cases where the person performing the transaction is a known terrorist or controlled by a known terrorist; cases in which the person performing the transaction is from a state that does not cooperate internationally to prevent money laundering and terrorist financing; and finally, transactions exceeding the currency reporting threshold that involve cash, property, securities, loans or remittances. If the total value of transactions conducted in one month exceeds set thresholds and there is reasonable evidence to suggest that the transactions are related, then all the transaction activity must be reported.

All remittances by law must be conducted through licensed banks. The government does not acknowledge alternative remittance systems. Currency exchange is allowed only through licensed currency exchange kiosks. All charities are registered with the Department of Humanitarian Assistance in the Presidential Administration. Charity assistance provided by foreign states, international organizations and individuals are regulated by Presidential Decree 24 passed in 2003 which requires all organizations and individuals receiving charity assistance to open charity accounts in a local bank.

Terrorism is a crime in Belarus and the AML Law establishes measures to prevent terrorism finance. Belarus' law on counterterrorism also states that knowingly financing or otherwise assisting a terrorist group constitutes terrorist activity. Under the Belarusian Criminal Code, the willful provision or collection of funds in support of terrorism by nationals of Belarus or persons in its territory constitutes participation in terrorism by aiding and abetting. In December 2005, the Belarusian Parliament amended the Criminal Code to stiffen the penalty for the financing of terrorism and thus bring Belarusian regulations into compliance with the International Convention for the Suppression of the Financing of Terrorism. The amendments explicitly define terrorist activities and terrorism finance and carry an eight to twelve year prison sentence for those found guilty of sponsoring terrorism. In February 2006, the Interior Ministry announced the establishment of a new counterterrorism department within its Main Office against Organized Crime and Corruption.

Belarusian legislation provides for broad seizure powers for law enforcement to identify and trace assets. Forfeiture is permitted in the Criminal Code for all serious offenses, including money laundering. Seizure of assets from third parties appears possible but is not specifically codified. The seizure of funds or assets held in a bank requires a court decision, a decree issued by a body of inquiry or pre-trial investigation, or a decision by the tax authorities.

A 2002 directive issued by the Board of Governors of the National Bank prohibits all transactions with accounts belonging to terrorists, terrorist organizations and associated persons. This directive also outlines a process for circulating to banks the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list. The National Bank is required to disseminate to banks the updates to the consolidated list and other information related to terrorist finance as it is received from the Ministry of Foreign Affairs. The directive gives banks the authority to freeze transactions in the accounts of terrorists, terrorist organizations and associated persons. In accordance with a resolution passed in March 2006, the Belarusian KGB compiled a list of 221 individuals suspected of participation in terrorism which the National Bank distributed to all domestic banks. Through 2007, Belarus has not identified any assets as belonging to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list.

Domestically, Belarus has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group established specifically to address these AML/CTF issues. This Working Group includes representatives of the Prosecutor's office, the National Bank, MTD, State Security Committee, Department of Financial Investigation, and the DFM. The Director of the DFM serves as the head of this Group.

Belarus has signed bilateral treaties on law enforcement cooperation with Afghanistan, Bulgaria, India, Latvia, Lithuania, the People's Republic of China, Poland, Romania, Syria, Turkey, the United Kingdom, and Vietnam. In September 2006, Belarus signed an AML agreement with the People's Bank of China. Belarus is also a party to five agreements on law enforcement cooperation and information sharing among CIS member states, including the Agreement on Cooperation among CIS Member States in the Fight against Crime and the Agreement on Cooperation among Ministries of Internal Affairs in the Fight against Terrorism. In 2004, Belarus joined the Eurasian Regional Group Against Money Laundering and the Financing of Terrorism (EAG), which is a FATF-style regional body (FSRB) with observer status in FATF. The DFM is a member of the Egmont Group, attaining membership in that body in May 2007. Belarus has also assumed international commitments to combat terrorism as a member of the Collective Security Treaty Organization (CSTO), which includes Armenia, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. In April 2007 the National Banks of Belarus and Kyrgyzstan signed an agreement on financial information exchange and training for fighting money laundering and terrorist financing.

Belarus is a party to the UN Convention against Corruption. In July 2006 President Lukashenko signed an anticorruption law to comply with the Council of Europe's 1999 Criminal Law Convention on Corruption, which Belarus ratified in 2004. In June 2007 Parliament passed Criminal Code amendments to toughen penalties for various offences by officials, including larceny through abuse of office, embezzlement, and legalization of assets illegally obtained. In July 2007 President Lukashenko issued an edict mandating the formation of specialized departments within prosecutors' offices, police stations and the KGB to fight against corruption and organized crime. Despite recent legislation, corruption remains a serious obstacle to enforcing laws dealing with financial crimes. Belarus ranked number 150 out of 180 territories listed in Transparency International's 2007 International Corruption Perception Index.

Belarus is a party to the 1988 UN Drug Convention, to the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism, though it has been actively expanding ties with Iran and Syria, both state sponsors of terrorism.

The Government of Belarus (GOB) has taken steps to construct a legal and regulatory framework to fight money laundering and terrorist financing. It should also focus on the implementation of the law by law enforcement, increasing the investigation and prosecution of money laundering and terrorist financing offenses. This could be accomplished through training and outreach by the FIU and other regulators. Belarus should increase the transparency of its business, finance, and banking sectors. Belarus' AML legislation should be amended to comport with international standards and to provide for more transparency and accountability. The GOB can accomplish this by extending the application of its current AML legislation to cover the governmental transactions that are currently exempted under the law, and ensure that the regulations and guidance provided by the National Bank and other regulators are legally binding. Similarly, the National Bank should be given the authority to carry out its responsibilities, and not be subject to influence by the Presidential Administration. The GOB should implement strict regulation on its industries operating abroad and on those operating within the FEZ areas. The GOB needs to reinstate the identification requirement for foreign currency exchange transactions, and reconsider the relationships it wishes to foster with state sponsors of terrorism. Belarus should continue to hone its guidance and enforcement of suspicious transaction reporting and provide adequate staff, tools, training and financial resources to its FIU so that it can operate

effectively, especially with the increased attention and reporting that the DFM has generated of late. The GOB must work to further improve the coordination between agencies responsible for enforcing AML measures. The GOB also needs to take steps to ensure that the AML framework operates more objectively and less as a political tool. The GOB should take serious steps to combat corruption in commerce and government.

Belgium

With assets of over \$2.5 trillion dollars in 2006, Belgium has a formidable banking industry. Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. However, the informal financial sector is particularly vulnerable to money laundering especially through the use of alternative remittance and underground banking. The diamond industry has also long been a sector of vulnerability. Belgian officials have also noted that criminals are increasing their use of the nonfinancial professions to facilitate access to the official financial sector.

Belgium criminalized money laundering through the Law of 11 January 1993, On Preventing Use of the Financial System for Purposes of Money Laundering. This law outlines customer due diligence and reporting requirements, which are also applicable to designated nonfinancial business and professions (DNFBPs). Obligated entities include estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, surveyors, and casinos. Additional laws make the requirements applicable to other sectors including credit institutions, investment firms, intermediaries, investment advisors and attorneys. The Belgian Banking and Finance Commission (CBFA) supervises financial institutions, including exchange houses, stock brokerages, and insurance companies. The Belgian Gaming Commission oversees casinos.

Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and nonfinancial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. Lawyers in particular do not consistently comply with reporting requirements. Belgian lawyers, for example, reported three suspicious transactions to the financial intelligence unit (FIU) in 2006. An association of Belgian lawyers has appealed the law to Belgium's court of arbitration on the grounds that it violates basic principles of the independence of the lawyer and of professional secrecy. Belgium is still awaiting a decision from the court of arbitration on this matter.

Article 505 of the Penal Code sets penalties of up to five years' imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense. Legislation implementing the Second European Union (EU) Directive on Money Laundering, or Council Directive 2001/97/EC On Prevention of the Use of the Financial System for Money Laundering, has broadened the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations.

The most recent mutual evaluation of Belgium was conducted by the Financial Action Task Force (FATF) in June 2005. Of the 49 recommendations, one of which was not applicable, Belgium received 41 ratings of "compliant" or "largely compliant." Although the report concluded that Belgium's anti-money laundering and counter-terrorist financing (AML/CTF) regime is effective, the assessment team found partial or noncompliance in some areas. These areas include: due diligence and regulation requirements for DNFBPs, licensing or registration of businesses providing money or value transfer services, allocation of adequate resources to the authorities charged with combating financial crimes, elimination of bearer bonds, development of an independent authority to freeze assets, and implementation of a system to monitor cross-border currency movements. Belgium is currently working to address these deficiencies.

Royal Decree of 5 October 2006, On Measures to Control Cross-border Transportation of Cash came into force on June 15, 2007. This decree implements regulation 1889/2005 of the EU Council on controls of cash entering or leaving the EU: travelers must declare transportation of currency into or out of the EU worth 10,000 euros (U.S. \$14,600) or more. In case of nondeclaration, or if there is a suspicion that the funds being declared originates from illegal activities or is intended to finance such activities, the Belgian Customs and Excise administration will confiscate the cash for a maximum period of 14 days and file a report. The Belgian FIU examines all the declarations and Customs reports that are filed. Since June 2007, Belgian Customs has received information on approximately 4.5 million euros (U.S. \$6.6 million) in cash being transported through Zaventem International Airport. To date, Belgian Customs has confiscated 670,000 euros (U.S. \$978,200) and filed eight reports with the FIU.

Belgian financial institutions must comply with “know your customer” principles, regardless of the transaction amount. Institutions must maintain records on the identities of clients engaged in transactions that are considered suspicious or that involve an amount equal to or greater than 10,000 euros (approximately U.S. \$14,650). Institutions must retain records of suspicious transactions reported to the FIU for at least five years. Financial institutions must train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Financial institutions or other entities with reporting requirements are also liable for illegal activities occurring under their control. Penalties for failure to comply with the AML legislation, including failure to report, include a fine of up to \$1.72 million.

Money laundering legislation imposes prohibitions on cash payments for real estate, except for an amount not exceeding 10 percent of the purchase price or 15,000 euros (U.S. \$21,900), whichever is lower. Cash payments over 15,000 euros (U.S. \$21,900) for goods are illegal.

Belgium has long permitted the issuance of bearer bonds (“titres au porteur”), widely used to transfer wealth between generations and to avoid taxes, for individuals as well as for institutions. In late 2005 the Belgian federal parliament adopted a law to cease the issuance of bearer bonds beginning on January 1, 2008. Bearer bonds issued before that date will still be valid, however, as well as nonBelgian bearer bonds.

Belgium needed to implement the Third EU Money Laundering Directive by December 15, 2007. The European Commission adopted recommendations for EU member states and a framework for a code of conduct for the nonprofit/charitable sector. Belgian officials are working to increase transparency in this sector through better enforcement of registration and reporting procedures. Requirements for nonprofit organizations include registering, furnishing copies of their statutes and lists of members, providing minutes from council meetings, and filing budget reports.

A growing problem, according to government officials, is the proliferation of illegal underground banking activities. Beginning in 2004, Belgian police made a series of raids on “phone shops”—small businesses where customers can make inexpensive phone calls and access the Internet. In some “phone shops,” authorities uncovered money laundering operations and hawala-type banking activities. In 2006, further raids uncovered numerous counterfeit phone cards and illegal or undocumented workers in addition to evidence of money laundering activities in some locations. Since 2004, the Belgian authorities have closed more than 150 “phone shops” and have estimated that the Belgian state may have been deprived of up to \$256 million in lost tax revenue each year through tax evasion by these businesses. Authorities report that “phone shops” often declare bankruptcy and later reopen under new management, making it difficult for officials to trace ownership and collect tax revenues. Authorities believe that 3,500 “phone shops” may be operating in Belgium. Only an estimated one-quarter of these shops have licenses to operate, and Belgian authorities are considering enforcing a stricter licensing regime. Some Brussels communes have also proposed heavy taxes on these types of shops in an effort to dissuade illegitimate commerce.

Belgium's robust diamond industry presents special challenges for law enforcement. Despite some decline in recent years, Belgium continues to be the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. Most of the "blood" or "conflict diamonds" from long-running African civil wars in the 1990s were processed in Antwerp. Authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and that office is examining the sector closely in cooperation with local police and diamond industry officials. Additionally, the Kimberley Process Certification Scheme (a joint government, international diamond industry, and civil society initiative designed to stem the flow of illicit diamonds) has introduced much-needed transparency into the global diamond trade. However, diamonds of questionable origin continue to appear on the Belgian market. The Government of Belgium (GOB) recognizes the particular importance of the diamond industry, as well as the potential vulnerabilities it presents to the financial sector. The GOB has distributed typologies outlining its experiences in pursuing money laundering cases involving the diamond trade, especially those involving the trafficking of African conflict diamonds. A regulation approved by a Royal Decree dated October 22, 2006 contains a detailed description of the required obligations for diamond dealers. This regulation primarily deals with the different aspects of client identification, including the identification of "nonface to face" operations and of the beneficial owner, customer due diligence, and obligations regarding the internal organization.

The Belgian financial intelligence unit (FIU), known in French as *Cellule de Traitement des Informations Financières* and in Flemish as *Cel voor Financiële Informatieverwerking* (CTIF-CFI), was created in June 1993. The FIU is an autonomous and independent public administrative authority, supervised by the Ministries of Justice and Finance. Institutions and persons subject to the reporting obligations fund the FIU. Although these contributions are compulsory, the contributing entities do not exercise any formal control over the FIU. CTIF-CFI's primary mission is to receive, analyze, and disseminate all suspicious transaction reports submitted by regulated entities. Operating as a filter between obligated entities and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. The financial sector cooperates actively with CTIF-CFI to guard against illegal activity. Institutions, their employees, and representatives are protected from civil, penal, or disciplinary actions when reporting transactions in good faith to CTIF-CFI. Legislation also exists to protect witnesses, including bank employees, who report suspicions of money laundering, or who come forward with information about money laundering crimes. Belgian officials have imposed sanctions on institutions or individuals that knowingly permitted illegal activities to occur. CTIF-CFI also acts as the supervisory body for professions not supervised by CBFA or other authorities. CTIF-CFI has analyzed the diamond industry and is working to eliminate its potential for money laundering and terrorist financing. It has initiated several meetings with the Belgian Ministry of Economic Affairs and the Antwerp World Diamond Center to clarify the obligations of diamond traders with respect to AML/CTF laws, and how diamond traders apply this legislation.

Financial experts, including three magistrates (public prosecutors) appointed by the King to a six-year renewable term of service, comprise the leadership of CTIF-CFI. A magistrate presides over the body. In addition to administrative and legal support, the investigative department consists of inspectors, analysts, three liaison police officers, one customs officer, and one officer of the Belgian intelligence service charged with maintaining contact with the various law enforcement agencies in Belgium.

In the first half of 2007, CTIF-CFI received 5,995 STRs and opened 2,301 case files, of which 551 were transmitted to the public prosecutor. By comparison, in 2006, the FIU received 9,938 disclosures, opened 3,367 new cases, and transmitted 912 cases to the public prosecutor. A breakdown of the 2007 figures was not available; but, in 2006, nearly 80 percent of disclosures on files transmitted to the federal prosecutor were made by credit institutions. Foreign exchange offices and foreign counterpart units accounted for an additional 15 percent of the files transmitted with notaries, casinos, and other

entities also reporting. The files concerning narcotics trafficking represented 15 percent of the total number of cases in 2006, while cases regarding terrorism and terrorist finance represented about four percent of the total number. The FIU reported 36 cases regarding terrorism or terrorist financing to the judicial authorities.

To date, Belgian courts have convicted 1,880 individuals for money laundering on the basis of cases forwarded by the FIU. These convictions have yielded combined total sentences of 2,819 years. Although five years is the maximum sentence for money laundering, the length of the sentence may increase if the financial crime is compounded by another type of crime such as drug trafficking. Belgian authorities have confiscated more than approximately \$788 million connected with money laundering crimes. The majority of convictions in relation to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

The federal police must also transmit suspected money laundering cases to the public prosecutor. In 2006 the federal police referred a total of 2,241 individuals to the public prosecutor for various crimes. More than 20 percent of these (450 individual cases) involved money laundering, fraud, and corruption. According to the FATF MER, the criminal prosecution authorities have the necessary power to carry out their functions; however, in some places or at some times, the prosecutors and police seem to lack resources to properly perform their AML/CTF duties.

The federal police enjoy good cooperation with their counterparts in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases. The federal police and the specialized services of the Central Office for the Fight against Organized Economic and Financial Crimes utilize a number of tactics to uncover money laundering operations, including investigating significant capital injections into businesses, examining suspicious real estate transactions, and conducting random searches at all international airports. In 2005, Project Cash Watch, carried out under the auspices of the federal police in Belgium's international airports and other transit venues, netted seizures of more \$2.45 million.

According to the FATF MER, Belgium has created a sophisticated and comprehensive confiscation and seizure regime, which includes the Central Office for Seizures and Confiscation (COSC). COSC operates under the auspices of the Ministry of Justice. Belgian law allows for criminal forfeiture of assets. A July 2006 law allows for the possibility, on a reciprocal basis, of the sharing of seized assets from serious crimes, including those related to narcotics, with affected countries. Since a judicial order is necessary before carrying out confiscations and seizures, COSC ensures that confiscations and seizures are executed smoothly and efficiently in accordance with Belgian law.

Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation to minimize the loss of the market value of the goods over time. If a suspect is later found innocent, he/she receives the cash equivalent of the item(s) sold, plus accrued interest. COSC has a commercial account for the deposit of confiscated funds. As of October 2007, the fund held more than \$165 million. COSC also maintains safe deposit boxes for the storage of high value items, such as jewelry. Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Noncash items are held in the clerks' offices in one of Belgium's 27 judicial districts. Indirect seizures are "seizures by equivalence," usually homes, cars, jewels, and other items of value not directly linked to the crime in question. Money from seizures and from the sale of seized goods is deposited into the Belgian Treasury.

Belgian legislation implementing the EU Council's Framework Decision on Combating Terrorism criminalizes terrorist acts and the provision of material and financial support for terrorist acts. It also allows judicial freezes on terrorist assets. The law followed the Second European Money Laundering Directive and also implemented eight of FATF's Special Recommendations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 specifically

penalizes the provision of material resources, including financial assistance, to terrorist groups; the penalty is five to ten years' imprisonment.

Under Belgium's AML/CTF law, bank accounts can be frozen on a case-by-case basis if there is sufficient evidence that a money laundering crime has been committed. The FIU has the legal authority to suspend a transaction for a period of up to two working days to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor.

The Ministry of Justice can freeze assets related to terrorist crimes. However, the burden of proof in such cases is relatively high. In order for an act to constitute a criminal offense, authorities must demonstrate that the target gave support knowing that it would contribute to the commission of a crime by the terrorist group. Because the law does not establish a national capacity for designating foreign terrorist organizations, Belgian authorities must demonstrate in each case that the group that received the support actually constitutes a terrorist group.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with Al-Qaida, the Taliban and Usama Bin Laden on the United Nations (UN) 1267 Sanctions Committee's consolidated list. It can also do so if the individual or entity is covered by an EU asset freeze regulation. Frozen assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, but not on the EU list, the GOB passes a ministerial decree to freeze assets to comply with the UN requirement. Assets of entities appearing on the EU list are automatically subject to a freeze without additional legislative or executive procedures. Belgium is working on legislation to permit the administrative freeze of terrorist assets in the absence of a judicial order or UN or EU designation.

Belgium's FIU is active with its colleagues in sharing information. CTIF-CFI has signed a memorandum of understanding with its United States counterpart that governs their collaborative work. CTIF-CFI was a founding member of the Egmont Group and headed the secretariat from 2005 to 2006. Belgium is a cooperative and reliable partner in law enforcement efforts as well.

Belgium is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Belgium has signed, but not yet ratified, the UN Convention against Corruption. A mutual legal assistance treaty (MLAT) between Belgium and the United States has been in force since January 2000, and an extradition treaty between the two countries has been operative since September 1997. Bilateral instruments amending and supplementing these treaties, in implementation of the U.S.-EU Extradition and Mutual Assistance Agreements, were signed with Belgium in December 2004, and await ratification, including by the U.S. side.

Belgium's continuing work on implementing the FATF recommendations complements an already solid AML regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. However, the Government of Belgium should continue to work through proposed legislation that pursues tougher and faster independent asset-freezing capability, as well as the optimal disposition of seized assets. The Government of Belgium should continue its efforts to uncover, investigate, and prosecute illegal banking operations, as well as increase attention to and dedicate more resources toward tracking the informal financial sector and nonbank financial institutions. This is especially applicable to the identification, regulation and enforcement of hawala enterprises that the GOB has already articulated as a concern. The GOB should strengthen adherence to reporting requirements by some nonfinancial entities in Belgium, such as lawyers and notaries, and enhance the regulations and reporting obligations for the nonprofit and charitable sector. To be even more effective in its efforts, Belgium may need to devote more resources, including investigative personnel, to police, prosecutors, and key Belgian agencies that work on money laundering, terrorist financing, and other financial crimes.

Belize

Belize is not a major regional financial center. In an attempt to diversify Belize's economic activities, authorities have encouraged the growth of offshore financial activities and have pegged the Belizean dollar to the U.S. dollar. Belize continues to offer financial and corporate services to nonresidents. Belizean officials suspect that money laundering occurs primarily within the country's offshore financial sector. Money laundering, primarily related to narcotics trafficking and contraband smuggling, is suspected to occur through banks operating in Belize. Criminal proceeds laundered in Belize are derived primarily from foreign criminal activities. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug-trafficking organizations, organized criminals or terrorist groups.

Offshore banks, international business companies, and trusts are authorized to operate from within Belize, although shell banks are prohibited within the jurisdiction. The Offshore Banking Act, 1996 governs activities of Belize's offshore banks. By law, offshore banks cannot serve customers who are citizens or legal residents of Belize. To legally operate from within Belize, all offshore banks must be licensed by the Central Bank and be registered with international business companies (IBCs). Before the Central Bank issues the license, the Central Bank must verify shareholders' and directors' backgrounds, ensure the adequacy of capital, and review the bank's business plan. The legislation governing the licensing of offshore banks does not permit directors to act in a nominee (anonymous) capacity.

Presently, there are eight licensed offshore banks, approximately 32,800 active registered IBCs, one licensed offshore insurance company, one mutual fund company, and 30 trust companies and agents operating in Belize. Only nonresident entities have access to offshore banks, and banks are not permitted to issue bearer shares. Local money exchange houses, which were suspected of money laundering, were closed effective July 2005. There is also an undisclosed number of Internet gaming sites operating from within the country. These gaming sites are unregulated at this time. Currently there are no offshore casinos operating from within Belize.

The International Business Companies Act of 1990 and its 1995 and 1999 amendments govern the operation of IBCs. The 1999 amendment to the Act allows IBCs to operate as banks and insurance companies. The International Financial Services Commission regulates the rest of the offshore sector. All IBCs must be registered. Although nonbank IBCs are allowed to issue bearer shares, the registered agents of such companies must know the identity of the beneficial owners of the bearer shares. Belize's legislation allows for the appointment of nominee directors of nonbank IBCs. The legislation for trust companies, the Belize Trust Act, 1992, is not as stringent as the legislation for other offshore financial services and does not preclude the appointment of nominee trustees.

There is one free trade zone presently operating in Belize, at the border with Southern Mexico. There are also designated free trade zones in Punta Gorda, Belize City, and Benque Viejo, but they are not operational. Data Pro Ltd. is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act. Commercial free zone (CFZ) businesses are allowed to conduct business within the confines of the CFZ, provided they have been approved by the Commercial Free Zone Management Agency (CFZMA) to engage in business activities. All merchandise, articles, or other goods entering the CFZ for commercial purposes are exempted from the national customs regime. However, any trade with the national customs territory of Belize is subject to the national Customs and Excise law. The CFZMA, in collaboration with the Customs Department and the Central Bank of Belize, monitors the operations of CFZ business activities. There is no indication the CFZ is presently being used in trade-based money laundering schemes or by financiers of terrorism.

Alternative remittance systems are illegal in Belize. However, Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial

institutions. Therefore, Belizean authorities monitor such activities at the borders with Mexico and Guatemala.

Allegedly, there is a significant black market for smuggled goods in Belize. However, there is no evidence to indicate that the smuggled goods are significantly funded by narcotics proceeds, or evidence to indicate significant narcotic-related money laundering. The funds generated from contraband are undetermined.

The Money Laundering (Prevention) Act (MLPA), in force since 1996 and amended in 2002, criminalizes money laundering related to many serious crimes, including drug trafficking, forgery, terrorism, blackmail, arms trafficking, kidnapping, fraud, illegal deposit taking, false accounting, counterfeiting, extortion, robbery, and theft. The minimum penalty for a money laundering offense as defined by the MLPA is three years imprisonment. Other legislation to combat money laundering includes the Money Laundering Prevention Guidance Notes; the Financial Intelligence Unit Act, 2002; the Misuse of Drugs Act; The International Financial Services Practitioners Regulations (Code of Conduct), 2001 (IFSPR); Money Laundering Prevention Regulations 1998 (MLPR); and the Offshore Banking Act, 2000, renamed the International Banking Act, 2002 (IBA).

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. The banking regulations governing offshore banks are different from the domestic banking regulations in terms of capital and operational requirements. Nevertheless, all licensed financial institutions in Belize (onshore and offshore) are governed by the same legislation and must adhere to the same anti-money laundering and counter-terrorist financing requirements. Government of Belize (GOB) officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, and counterfeit Belizean and United States currency. The Central Bank of Belize has engaged in public awareness activities and training sessions to regulate counterfeit currency.

The Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to establish due diligence (“know-your-customer”) provisions, monitor their customers’ activities and report any suspicious transaction to the financial intelligence unit (FIU) of Belize. Belize law obligates banks and other financial institutions to maintain business transactions records for at least five years when the transactions are complex, unusual or large. Money laundering controls are also applicable to nonbank financial institutions, such as exchange houses, insurance companies, lawyers, accountants and the securities sector, which are regulated by the International Financial Services Commission. Financial institution employees are exempt from civil, criminal or administrative liability for cooperating with regulators and law enforcement authorities in investigating money laundering or other financial crimes. Belize does not have any bank secrecy legislation that prevents disclosure of client and ownership information.

The reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than \$10,000 in cash or negotiable instruments are required to file a declaration with the authorities at Customs, the Central Bank and the FIU.

The FIU of Belize, established in 2002, is an independent agency presently housed at the Central Bank. Current laws do not provide for the funding of the FIU, and the FIU has to apply to the Ministry of Finance for funds. Due to financial constraints, the FIU is not adequately staffed and existing personnel lack sufficient training and experience. In November 2005, the director of the FIU resigned, leaving the FIU with only four employees; the new FIU director did not begin until July 2006. In December 2007, both the financial examiner and the office attendant resigned from their posts. According to the FIU’s office manager, however, replacements for both employees have already been identified.

The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU also has administrative, prosecutorial and investigative responsibilities for financial crimes, such as money laundering and terrorist financing. The FIU received 38 suspicious transaction reports (STRs) from obligated entities in 2007, nine of which became the subject of investigations. In 2007, there were press reports indicating a possible money laundering scheme by a former public official, but no subsequent investigation was conducted. Overall there were no major money laundering cases to report in 2007, and the anti-money laundering regime in Belize remains relatively ineffective.

Although the FIU has access to records and databanks of other GOB entities and financial institutions, there are no formal mechanisms for the sharing of information with domestic regulatory and law enforcement agencies. However, the FIU is empowered to share information with FIUs in other countries. On several occasions, the FIU has cooperated with the United States.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering or terrorist financing are treated as criminal forfeitures. The banking community cooperates fully with enforcement efforts to trace funds and seize assets. The FIU and the Belize Police Department are the entities responsible for tracing, seizing and freezing assets, and the Ministry of Finance can also confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze, and seize assets related to money laundering or terrorist financing. Currently, the GOB's legislation does not specify the length of time assets can be frozen. There are no limitations to the kinds of property that may be seized, and any property—tangible or intangible—that may be related to a crime or is shown to constitute the proceeds of a crime, including legitimate businesses, may be seized. However, Belizean law enforcement lacks the resources necessary to effectively trace and seize assets.

GOB authorities are considering the enactment of a Proceeds of Crime law, which will address the seizure or forfeiture of assets of narcotics traffickers, financiers of terrorism, or organized crime. Currently, the GOB is not engaged in any bilateral or multilateral negotiations with other governments to enhance asset tracing and seizure. However, the GOB cooperates with the efforts of foreign governments to trace or seize assets related to financial crimes.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation, The Money Laundering (Prevention) (Amendment) Act, 2002. GOB authorities have circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to all financial institutions in Belize. There are no indications that charitable or nonprofit entities in Belize have acted as conduits for the financing of terrorist activities. Consequently, the country has not taken any measures to prevent the misuse of charitable and nonprofit entities from aiding in the financing of terrorist activities.

Belize has signed and ratified a Mutual Legal Assistance Treaty with the United States, which provides for mutual legal assistance in criminal matters and entered into force in 2003. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance to authorities of other jurisdictions in matters pertaining to money laundering and other financial crimes. Belize is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. The GOB has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. Belize is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group of financial intelligence units in 2004.

The Government of Belize should ensure effective implementation of its anti-money laundering and counter-terrorist financing regime. The GOB should increase resources to provide adequate staffing levels and training to those entities responsible for enforcing Belize's anti-money laundering and counter-terrorist financing laws, including the financial intelligence unit and the asset forfeiture regime. Belize should take steps to address the vulnerabilities in its supervision of its offshore sector, particularly the lack of supervision of the gaming sector, including Internet gaming facilities. Belize should immobilize bearer shares and ensure that the offshore sector complies with anti-money laundering and counter-terrorist financing reporting requirements. The GOB should also become a party to the UN Convention against Corruption.

Bolivia

Although Bolivia is not a regional financial center, money laundering activities related to public corruption, contraband smuggling, trafficking in persons, and narcotics trafficking continue to be vulnerabilities. Bolivia's long tradition of bank secrecy and the lack of effective government oversight of nonbank financial activities facilitate the laundering of the profits of organized crime and narcotics trafficking, evasion of taxes, and the laundering of other illegally obtained earnings.

Bolivia's financial sector consists of approximately 13 commercial banks, six private financial funds, nine mutual funds, 23 savings and credit cooperatives, 14 insurance companies and one stock exchange, all of which are subject to the same anti-money laundering controls. The Bolivian financial system is highly dollarized, with approximately 69 percent of deposits and 81 percent of loans distributed in U.S. dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of El Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre, and Desaguadero.

Many entities that move money in Bolivia remain unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses are known to transfer money freely into and out of Bolivia but are not subject to anti-money laundering controls. Informal exchange businesses, particularly in the department of Santa Cruz, also transmit money to avoid law enforcement scrutiny.

Law 1768 of 1997 criminalizes money laundering in Bolivia. Law 1768 modifies the penal code; criminalizes money laundering related only to narcotics trafficking, organized criminal activities and public corruption; provides for a penalty of one to six years for money laundering; and defines the use of asset seizure beyond drug related offenses. However, the law cannot be applied unless the prosecution demonstrates in court that the accused participated in and was convicted of the predicate offense. Law 1768 also created Bolivia's financial intelligence unit (FIU), the Unidad de Investigaciones Financieras (UIF), within the Office of the Superintendence of Banks and Financial Institutions. Supreme Decree 24771 of 1997 defines the attributes and functions of the UIF.

As Bolivia's FIU, the UIF is responsible for collecting and analyzing data on suspected money laundering and other financial crimes, and sharing this information with the Bolivian National Police and the Public Ministry (Attorney General's Office) as appropriate. Decree 24771 requires banks, insurance companies, and securities brokers to identify their customers, retain records of every transaction for a minimum of ten years, and report to the UIF all transactions that are considered unusual (without apparent economic justification or licit purpose) or suspicious (customer refuses to provide information or the explanation and/or documents presented are clearly inconsistent or incorrect). There is no requirement for obligated entities to report cash transactions above a designated threshold under the current law, and no requirement exists stating that persons entering or leaving the country declare the transportation of currency over a designated threshold. However, the UIF may request additional information from obligated financial institutions to assist prosecutors with their investigations.

The UIF is responsible for implementing anti-money laundering controls, and may request that the Superintendent of Banks sanction obligated institutions for noncompliance with reporting requirements. The UIF also conducts on-site inspections of obligated entities to review their compliance with the reporting of suspicious transactions. Given the size of Bolivia's financial sector, compliance with reporting requirements is extremely low, with the UIF receiving an average of 50 suspicious transaction reports (STRs) per year. According to the UIF, banks in Bolivia were reporting more frequently in 2007: in the first six months of 2007, the UIF received 60 STRs. The UIF is currently reviewing a total of 110 reports.

The Special Group for Investigation of Economic Financial Affairs (GIAEF) was created in 2002 within Bolivia's Special Counter-Narcotics Force (FELCN) and is responsible for investigating narcotics-related money laundering cases. Currently, there are three GIAEF units in Bolivia with a total of 27 personnel. The GIAEF reported 26 money-laundering investigations and over \$9 million in assets seized over the last 12 months. The GIAEF, UIF, Public Ministry, National Police, and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information.

Corruption remains a serious issue in Bolivia. According to 2006 estimates by the U.S. Agency for International Development (USAID), corruption costs Bolivians approximately \$115 million per year. Traditionally, allegations against high-ranking law enforcement officials were routinely dismissed or forgotten. However, recent anti-corruption laws increased the effectiveness of investigations and the number of cases related to corruption is growing. The Office of Professional Responsibility (OPR) of the National Police has investigated a total of 1,779 cases involving allegations of misconduct and/or impropriety alleged against police officers. Of these, 205 cases were investigated involving police officers assigned to FELCN. Of these 205 cases involving FELCN officers, however, none resulted in findings of corruption.

To further combat corruption, the Government of Bolivia (GOB) promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, in April 2006. Among a number of other provisions, the decree provides for the creation of a "Financial and Property Intelligence Unit," which would replace the UIF. Decree 28695 originally repealed Decree 24771, which gave the UIF its authority. However, because the repeal of Decree 24771 would eliminate the UIF before its replacement was operational, the GOB passed Decree 28956 in November 2006, eliminating the portion of Decree 28695 that had repealed Decree 24771 and allowing the UIF to continue to operate until the Financial and Property Intelligence Unit becomes a functioning entity.

As a result of the new decree and the plans to establish the Financial and Property Intelligence Unit, the UIF has lost a number of staff, bringing the number of personnel down to only five. Limitations in its reach, a lack of resources, and weaknesses in its basic legal and regulatory framework have hampered the UIF's effectiveness as a financial intelligence unit. There is no indication that the establishment of the Financial and Property Intelligence Unit will resolve these problems and allow for a more effective UIF.

In addition to Decrees 28695 and 28956, the Constitutional Commission of the Bolivian Chamber of Deputies is considering two competing anti-money laundering bills. Although the draft law provides a mission for the Financial and Property Intelligence Unit, there are concerns regarding the functions and authorities of the new entity, as its primary function would be to investigate cases of corruption rather than money laundering. The law also does not criminalize "self-laundering," meaning that a person could only be convicted of money laundering if he/she launders the funds generated by a crime committed by a third party. In general, the law does not include provisions to bring Bolivia's anti-money laundering regime into greater compliance with international standards, in spite of suggestions and input from the Financial Action Task Force for South America (GAFISUD), the International

Monetary Fund (IMF), the UIF, and the Government of the United States. The draft was presented to Chamber of Deputies in early December 2006, but the Chamber has not acted on it.

The second draft anti-money laundering law addresses more of the deficiencies in Bolivia's current level of compliance with the international standards for combating money laundering. This draft criminalizes self-laundering, permits special investigative techniques, and prohibits bank secrecy. This draft expands predicate offenses for money laundering beyond the three current offenses, but they are still limited to a list of specific offenses, rather than all serious crimes. Although the bill establishes terrorist financing as a predicate offense for money laundering, terrorist financing is not a crime in Bolivia. The draft law expands the number of obligated entities (to include exchange houses and money remitters); but other entities that are required to be regulated under the Financial Action Task Force (FATF) standards, such as dealers in precious metals and jewels, are not included. The draft law also does not provide legal protection for obligated entities when filing STRs or responding to requests for information from the UIF.

There are also concerns that the new legislation will not improve the GOB's overall anti-money laundering regime, which is undermined by the lack of a legal and bureaucratic framework for money laundering investigations. To prosecute a money laundering case, Bolivian law requires that the crime of money laundering be charged alongside an underlying predicate offense. Although the Public Prosecutors are responsible for prosecuting money laundering offenses, they do not have a specialized dedicated unit. Judges trying these cases are challenged to understand their complexities. To date, there has been only one conviction involving money laundering.

There are also serious deficiencies in Bolivia's legal framework with regard to civil responsibility. Under Bolivian law, there is no protection for judges, prosecutors or police investigators who make good-faith errors while carrying out their duties. If a case is lost initially or on appeal, or if a judge rules that the charges against the accused are unfounded, the accused can request compensation for damages, and the judges, prosecutors, or investigators can be subject to criminal charges for misinterpreting the law. This is particularly problematic for money laundering investigations, as the law is full of inconsistencies and contradictions, and is open to wide interpretation. For these reasons, prosecutors are often reluctant to pursue these types of investigations.

While traditional asset seizure continues to be employed by counternarcotics authorities, until recently the ultimate forfeiture of assets was problematic. Prior to 1996, Bolivian law permitted the sale of property seized in drug arrests only after the Supreme Court confirmed the conviction of a defendant. A 1995 decree permitted the sale of seized property with the consent of the accused and in certain other limited circumstances. The Directorate General for Seized Assets (DIRCABI) is responsible for confiscating, maintaining, and disposing of the property of persons either accused or convicted of violating Bolivia's narcotics laws. DIRCABI, however, has been poorly managed for years, and has only auctioned confiscated goods sporadically. In 2007, DIRCABI submitted a draft decree proposing changes in the existing law and procedures relating to asset seizure, forfeiture, and sharing. The President signed Decree 29305 on October 10, 2007. However, the decree does not correct problems related to the sharing of forfeited assets among law enforcement entities. DIRCABI initiated 485 cases in the first six months of 2007, with 16 bank accounts containing over \$4 million subject to seizure or forfeiture.

The UIF, with judicial authorization, may also freeze accounts for up to 48 hours in suspected money laundering cases. To date, this law has only been applied on one occasion.

Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB currently lacks legislation that criminalizes the financing of terrorism or grants the GOB the authority to identify, seize, or freeze terrorist assets. Nevertheless, the UIF distributes the terrorist lists of the United Nations and the United States, receives and maintains information on terrorist groups, and can freeze suspicious assets under its own authority for up to 48 hours, as it has done in counternarcotics cases.

The UIF created a draft terrorist financing law in 2006 and presented it to the Superintendence of Banks. However, the bill has not yet been presented to Congress.

The GOB's lack of terrorist financing legislation resulted in Bolivia's suspension from the Egmont Group of financial intelligence units on July 31, 2007. The Egmont Group amended its membership requirements in June 2004, requiring all member states to criminalize the financing of terrorism and their FIUs to receive STRs related to terrorist financing. Existing members, which included Bolivia, were given until June 2007 to draft terrorist financing legislation. Bolivia was the only Egmont member that had not drafted legislation by the deadline and as a result, the UIF was suspended from the Egmont Group. The suspension bars the UIF from participating in Egmont meetings or using the Egmont Secure Web (the primary means of information exchange among Egmont members) to share information with other FIUs. If the GOB does not take significant steps towards the criminalization of terrorist financing by June 2008, the UIF will be expelled from the Egmont Group.

The GOB is a member of GAFISUD, and its most recent mutual evaluation was conducted in April 2006. As a result of the GOB's failure to pay its membership dues for the past three years, GAFISUD placed sanctions on Bolivia in July and suspended its membership on December 1, 2007. The GOB made a partial payment of its arrears immediately following its December 1 suspension. At its December plenary meeting, GAFISUD agreed to reinstate Bolivia's membership, on the condition that the remainders of its debts are paid by July 2008. As a result of GAFISUD members' concerns regarding the GOB's failure to meet the FATF standards on combating money laundering and terrorist financing, the GAFISUD Secretariat sent a high level delegation to meet with senior GOB officials in November 2007.

Bolivia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. Bolivia is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. The GOB has signed, but not ratified, the Inter-American Convention against Terrorism. The GOB and the United States signed an extradition treaty in June 1995, which entered into force in November 1996.

While the Government of Bolivia is taking some necessary steps to combat corruption, the GOB should ensure that any changes in its anti-corruption legislation strengthen its anti-money laundering regime. The GOB should also improve its current money laundering legislation so that it conforms to the standards of the FATF and GAFISUD. Money laundering should be an autonomous offense without requiring prosecution for the underlying predicate offense, and currently unregulated sectors should be subject to anti-money laundering and counter-terrorist financing controls. The GOB should criminalize terrorist financing in a timely manner and allow for the blocking of terrorist assets, to fulfill its international obligations. Doing so will also ensure that the UIF is not expelled from the Egmont Group. In addition to the need to make significant changes to the current laws, Bolivia should also ensure that the UIF and its potential replacement have sufficient staff and resources. The UIF should also have the authority to receive suspicious transaction reports on activities indicative of terrorist financing and reports from nonbank financial institutions. The GOB should also pay its GAFISUD dues to avoid being suspended from GAFISUD again. Finally, Bolivia needs to strengthen the relationships and cooperation between all government entities involved in the fight against money laundering and other financial crimes.

Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) has a cash-based economy and is not an international, regional, or offshore financial center. The laundering of illicit proceeds derives from criminal activity including the proceeds from smuggling, corruption, and widespread tax evasion. Due to its porous borders and

weak enforcement capabilities, BiH is a significant market and transit point for illegal commodities including cigarettes, narcotics, firearms, counterfeit goods, lumber, and fuel oils. BiH authorities have had some success over the past few years in clamping down on money laundering through the formal banking system. There are four active Free Trade Zones in BiH, with production based mainly on automobiles and textiles.

There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina and the Republika Srpska), and Brcko District. The Federation is further divided into ten cantons. Criminal and criminal procedure codes from the State, the two entities, and Brcko District were enacted and harmonized in 2003, although jurisdictions maintain their own enforcement bodies. Although state-level institutions are becoming more firmly grounded and are gaining increased authority, there remains a fair amount of confusion regarding jurisdictional matters between the entities and state-level institutions. Unless otherwise specified, relevant laws and institutions are at the state level.

Money laundering is a criminal offense in all state and entity criminal and criminal procedure codes. At the state level, the Law on the Prevention of Money Laundering determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. The law also prescribes measures and responsibilities for international cooperation and establishes a financial intelligence unit (FIU) within the State Investigative and Protection Agency (SIPA). The law requires banks to submit suspicious financial transactions to the state-level FIU. Those convicted of money laundering exceeding the equivalent of \$30,000 receive prison terms between one and ten years. For lesser amounts, the penalty is imprisonment between six months and five years.

The Law on the Prevention of Money Laundering requires twenty-six types of entities to report to the FIU all transactions of U.S. \$18,000 or more as well as all transactions (regardless of amount) suspected of connections to money laundering or terrorist financing. The money laundering law applies to all banks, individuals and several nonbank financial institutions including post offices, investment and mutual pension companies, stock exchanges and stock exchange agencies, insurance companies, casinos, currency exchange offices and intermediaries such as lawyers and accountants. In addition to cash and suspicious transaction reporting requirements, the law requires that customs officials from the Indirect Tax Authority (ITA) forward to the FIU all reports of cross-border transportation of cash and securities in excess of \$6,000. All banks have the ability to send electronic cash transaction reports (CTRs) and suspicious transactions reports (STRs) to the FIU, which then stores them in a central database. Although the law places reporting obligations on twenty-six types of entities, the banking sector and the ITA file the majority of reports, leaving a majority of the nonbank sector even more vulnerable to money laundering.

BiH has not enacted bank secrecy laws that prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities. The law requires banks and other financial institutions to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above the equivalent of \$18,000. Financial institutions must maintain records for twelve years to respond to law enforcement requests. Bosnian law protects reporting individuals with respect to law enforcement cooperation. Although there is no state-level banking supervision agency, entity level banking supervision agencies oversee and examine financial institutions for compliance with anti-money laundering and counter-terrorist financing laws and regulations. There is, however, no formal supervision mechanism in place for nonbank financial institutions and intermediaries. Nonbank financial transfers are reportedly very difficult for law enforcement and customs officials to investigate. This is due not only to a lack of reporting, but also to a lack of understanding of indigenous methodologies, many of which are found in the underground economy and are enabled by smuggling and the misuse of trade .

Police at both the state and entity levels investigate financial crimes. At the state level, SIPA and the FIU are responsible for investigating financial crimes. In addition, the Federation Police has an Economic Crime Unit which focuses on public corruption, economic crimes, money laundering, and cyber crime. Although Republika Srpska (RS) police also investigate financial crimes, they do not have a specialized unit to handle such crimes. Both the Federation Police and the RS police lack adequate resources and training. In addition, both agencies acknowledge that the level of cooperation and information exchange with SIPA is poor and needs improvement.

The ITA suffers from a lack of resources and sufficiently trained personnel. BiH is largely a cash economy, and it is typical to carry large amounts of cash, even across borders. Bosnia and Herzegovina also receives significant remittances from emigrants. Official remittances constitute over 20 percent of GDP. While some of this will come into the country through bank transfers, others will also cross the border via courier.

The Financial Intelligence Department (FID), Bosnia-Herzegovina's FIU, is a hybrid body, performing analytical duties while maintaining limited criminal investigative responsibilities. The FID receives, collects, records, analyzes, and forwards information related to money laundering and terrorist financing to the State Prosecutor. It also provides expert support to the Prosecutor regarding financial activities and handles international cooperation on money laundering issues. Officially, the FID has access to the records of other government entities and formal mechanisms for inter-agency information sharing are in place. In practice, however cooperation between the FID and other government agencies is weak, with little information shared among agencies. This applies particularly to information sharing between the FID and the different police forces, as the banking agencies do share information with the FID. When suspicion of illicit activity exists, the FID has the power to freeze accounts for five days. During this time, if the FID is able to collect sufficient evidence of possible criminal activity, it may forward the case to the Prosecutor. At that point, the freeze on the accounts may be extended. The FID reports that it froze KM 752,439 (approximately U.S. \$537,456) in six different cases during the first nine months of 2007.

The September 2006, International Monetary Fund's Financial System Stability Assessment report praised Bosnia Herzegovina for the progress made since MONEYVAL's 2005 mutual evaluation report. It cited in particular "the development of an effective state-level FIU." This has been augmented by the FID's hiring and training of several new analysts in late 2006. The report also cited the problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies.

In the first nine months of 2007, FID received 195,170 currency reports from banks and other financial institutions. Of these, the FID identified 57 cases as suspicious and investigated them. The FID submitted 12 reports to the BiH Prosecutor—eight related to money laundering and four related to other crimes such as abuse of position and tax evasion. Since BiH established its AML regime, there have been 28 confirmed convictions for money laundering. The FID is not the only active agency in the regime: the RS entity police agency and the Federation Financial Police, among others, all reported cases. In the first nine months of 2007, Bosnia-Herzegovina had seven convictions for money laundering.

BiH has no specific asset forfeiture law as regards money laundering, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws which allow for the seizure of PIFWC assets or assets of those providing material support to them. Articles 110 and 111 of the BiH Criminal Code (along with similar laws in the harmonized entity and Brcko Criminal Codes) are the only legal provisions that authorize asset forfeiture. These provisions authorize the "confiscation of material gain" (or a sum of money equivalent to the material gain if confiscation is not feasible) from illegal activity. The law does not provide for the seizure and forfeiture of assets that may have been used or facilitated the commission of the illegal activity. The courts administer confiscation, which can only

take place as part of a verdict in a criminal case. The courts decide whether the articles will be “sold under the provisions applicable to judicial enforcement procedure, turned over to the criminology museum or some other institution, or destroyed. The proceeds obtained from sale of such articles shall be credited to the budget of Bosnia and Herzegovina.” Prosecutors and courts do not have the administrative mechanisms in place to seize assets, maintain them in storage, dispose of them, or route the proceeds to the appropriate authorities. The government may seize property as punishment for criminal offenses for which a term of imprisonment of five years or more is prescribed. In such cases, asset seizure is possible without proving a specific relationship between the assets and the crime. There is no mechanism for civil forfeiture. There are no laws for sharing seized assets with other governments. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist-finance-related and other assets. The banking agencies (Federation and RS Banking Agencies) in particular have the capability to freeze assets without undue delay. The banking community cooperates with law enforcement efforts to trace funds and freeze accounts.

Article 202 of the criminal procedure code criminalizes terrorist financing. BiH is a party to the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Entity banking agencies are cognizant of the requirements to sanction individuals and entities listed by the UNSCR 1267 Sanctions Committee’s consolidated list, but the state authorities do not regularly circulate this list to entity authorities. The U.S. Embassy, however, provides updates to appropriate entity authorities

In 2006, after a cooperative investigation between BiH and law enforcement authorities in several European Union countries, authorities initiated a prosecution at the Court of Bosnia and Herzegovina against five people suspected of terrorist crimes. Four of the defendants were found guilty in January 2007, and this verdict was affirmed by a three-judge appellate panel of the BiH State Court in June, making the verdict final and binding. In 2004, the government disrupted the operations of Al Furqan (aka Sirat, Istikamet), Al Haramain & Al Masjed Al Aqsa Charity Foundation, and Taibah International, organizations listed by the UNSCR 1267 Committee as having direct links with al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing.

Bosnia and Herzegovina has no Mutual Legal Assistance Treaty with the U.S. BiH succeeded to the extradition treaty concluded between the Kingdom of Serbia and the United States in 1902; while this treaty covers some financial crimes, it does not address contemporary forms of money laundering. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings. Authorities have made good faith efforts to exchange information informally with officials from the United States. BiH is a party to the 1988 UN Drug Convention (by way of succession from the former Yugoslavia), the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism. Unfortunately, on many occasions, BiH has not passed implementing legislation for the international conventions to which it is a signatory.

The Government of Bosnia and Herzegovina (GOBH) should continue to strengthen institutions with responsibilities for money laundering prevention, particularly those at the state level. Due to a lack of resources and bureaucratic politics, SIPA and the FID, like many state institutions, remain under funded and under-resourced. The GOBH should make efforts to increase funding for its AML/CTF programs and enhance cooperation between concerned departments and agencies. Although prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering and other financial crimes, the GOBH should provide training to ensure that they understand diverse methodologies and aggressively pursue investigations. BiH authorities should undertake efforts to understand the illicit markets and their role in trade-based money laundering and alternative remittance systems. The banking agencies in BiH need to increase awareness by improving

outreach programs with respect to compliance with AML/CTF regulations. Major vulnerabilities that they should address include the identification of shell companies and beneficial owners as well as the monitoring of NGO's. In addition, GOBH should implement a formal supervisory mechanism for nonbank financial institutions and intermediaries. The adoption of such a mechanism would help increase reporting in the nonbank sector, thereby reducing the vulnerability to money laundering that currently exists in that sector. BiH law enforcement and customs authorities should take additional steps to control the integrity of the border and limit smuggling. BiH should study the formation of centralized regulatory and law enforcement authorities and take specific steps to combat corruption at all levels of commerce and government. BiH should also adopt a comprehensive asset forfeiture law which provides a formal mechanism for the administration of seized assets, and should consider establishing a civil forfeiture regime. The government should enact implementing legislation for the international conventions to which it is a signatory

Brazil

Brazil is the world's fifth largest country in both size and population, and its economy is the tenth largest in the world. Due to its size and significant economy, Brazil is considered a regional financial center, although it is not an offshore financial center. Brazil is also a major drug-transit country. Brazil maintains adequate banking regulations, retains some controls on capital flows, and requires disclosure of the ownership of corporations. Brazilian authorities report that money laundering in Brazil is primarily related to domestic crime, especially drug trafficking, corruption, organized crime, and trade in contraband, all of which generate funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. However, use of the Brazilian financial system to launder the proceeds of foreign criminal activity also persists. For example, Colombian narcotics trafficker Juan Carlos Ramirez Abadia, who is currently pending extradition to the United States, laundered millions in Norte Valle drug cartel proceeds through Brazil.

A primary source of criminal activity and contraband is the Tri-Border Area (TBA) shared by Argentina, Brazil, and Paraguay. Brazilian authorities have expressed particular concern over the trafficking in arms and drugs in the TBA. Brazilian authorities note that the proceeds of domestic drug trafficking and organized crime feed a regional arms trade, operating in the TBA. In addition, a wide variety of counterfeit goods, including cigarettes, compact discs (CDs), digital versatile discs (DVDs), and computer software, are smuggled across the border from Paraguay into Brazil; a significant portion of these counterfeit goods originate in Asia. The U.S. Government believes the TBA to be a source of terrorist financing, although the Government of Brazil (GOB) maintains that it has not seen any evidence of such. In recent years, the GOB has enhanced its border controls in the TBA, particularly at the Foz do Iguacu border crossing, in an attempt to combat the significant inflow of contraband goods and subsequent tax revenue loss.

The GOB has a comprehensive anti-money laundering regulatory regime in place. Law 9.613 of 1998 criminalizes money laundering related to drug trafficking, terrorism, arms trafficking, extortion by kidnapping, crimes against the public administration or the national financial system, and organized crime, and penalizes offenders with a maximum of 10 years in prison. The law expands the GOB's asset seizure and forfeiture provisions, and exempts "good faith" compliance from criminal or civil prosecution. Regulations issued in 1998 require that individuals transporting more than 10,000 reais (then approximately U.S. \$10,000, now approximately U.S. \$5,500) in cash, checks, or traveler's checks across the Brazilian border must fill out a customs declaration that is sent to the Central Bank.

Law 10.467 of 2002, which modifies Law 9.613, put into effect Decree 3.678 of 2000, thereby penalizing active corruption in international commercial transactions by foreign public officials. Law 10.467 also adds penalties for this offense under Chapter II of Law 9.613. Law 10.701 of 2003, which also modifies Law 9.613, establishes terrorist financing as a predicate offense for money laundering.

The law also establishes crimes in foreign jurisdictions as predicate offenses, requires the Central Bank to create and maintain a registry of information on all bank account holders, and enables the Brazilian financial intelligence unit (FIU) to request from all government entities financial information on any subject suspected of involvement in criminal activity.

Law 9.613 establishes Brazil's FIU, the Conselho de Controle de Atividades Financeiras (COAF), which is housed within the Ministry of Finance. The COAF includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police. The COAF regulates those financial sectors not already under the jurisdiction of another supervising entity. Currently, the COAF has a staff of 42, comprised of 20 analysts, two international organizations specialists, a counterterrorism specialist, two lawyers, and support staff.

Since 1999, the COAF has issued a series of regulations that require customer identification, record keeping, and reporting of suspicious transactions to the COAF by obligated entities. Entities that fall under the regulation of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC) file suspicious activity reports (SARs) with their respective regulator, either in electronic or paper format. The regulatory body then electronically submits the SARs to COAF. Entities that do not fall under the regulations of the above-mentioned bodies, such as real estate brokers, money remittance businesses, factoring companies, gaming and lotteries, dealers in jewelry and precious metals, bingo, credit card companies, commodities trading, and dealers in art and antiques, are regulated by the COAF and send SARs directly to COAF, either via the Internet or using paper forms.

In addition to filing SARs, banks are also required to report cash transactions exceeding 100,000 reais (approximately \$55,000) to the Central Bank. The lottery sector must notify COAF of the names and data of any winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. COAF Resolution 14 of 2006 further extended these anti-money laundering requirements to the real estate sector. The insurance regulator, SUSEP, clarified its reporting requirements for insurance companies and brokers in Circular 327 of May 2006, which requires these entities to have an anti-money laundering program and report large insurance policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF. In addition, on January 8, 2008, the Securities Commission (CVM) extended anti-money laundering requirements to additional entities, including luxury goods dealers and persons or companies that conduct business activities involving a large volume of cash.

Since 2006, the COAF, Central Bank, SUSEP, and the Pension Funds Secretariat have issued resolutions and circulars mandating the reporting of suspected terrorist financing activity, and the reporting of suspicious or large cash transactions by politically exposed persons (PEPs). The Central Bank issued Circular 3339 in December 2006, defining procedures for monitoring the financial accounts of PEPs. SUSEP Circular 21 of December 2006 addresses reporting procedures for transactions and possible transactions linked to terrorism and terrorist financing. SUSEP Circular 341, issued April 30, 2007, amends Circular 327 of May 2006, and includes procedures to be observed regarding PEPs. On March 28, 2007, COAF issued Resolutions 15 and 16, which respectively expand reporting requirements regarding suspected terrorist financing and transactions by PEPs. The Pension Funds Secretariat published new rules on PEPs on December 11, 2007, through Circular Letter SPC 18/2007.

The COAF has direct access to the Central Bank database, so that it has immediate access to the SARs and cash transaction reports (CTRs) filed with the Central Bank. The COAF also has access to a wide variety of government databases. The COAF may request additional information directly from the entities it supervises and the supervisory bodies of other obligated entities. Complete bank transaction information may be provided to government authorities, including the COAF, without a court order. Domestic authorities that register with the COAF may directly access the COAF databases via a

password-protected system. In 2007, the COAF received 50,320 CTRs and 18,960 SARs per month. In 2007, the COAF sent 1,555 reports to law enforcement authorities for further investigation, and responded to 1,047 requests for information received from law enforcement and prosecutorial authorities in the last year.

The Central Bank has established the Departamento de Combate a Ilícitos Cambiais e Financeiros (Department to Combat Exchange and Financial Crimes, or DECIC) to implement anti-money laundering policy, examine entities under the supervision of the Central Bank to ensure compliance with suspicious transaction reporting, and forward information on the suspect and the nature of the transaction to the COAF. In 2005, the DECIC brought on-line a national computerized registry of all current accounts (e.g., checking accounts) in the country. The COAF also has access to this database. Banks must report identifying data on both parties for all foreign exchange transactions and money remittances, regardless of the amount of the transaction.

The GOB has institutionalized its national strategy for combating money laundering, holding its fifth annual high-level planning and evaluation session in November 2007. At these sessions, the GOB defines annual goals within the scope of its overall strategy that aims to advance six strategic goals: improve coordination of disparate federal and state level anti-money laundering efforts, utilize computerized databases and public registries to facilitate the fight against money laundering, evaluate and improve existing mechanisms to combat money laundering, increase international cooperation to fight money laundering and recover assets, promote an anti-money laundering culture, and prevent money laundering before it occurs. The national anti-money laundering strategy has put in place more regular coordination and clarified the division of labor among various federal agencies involved in combating money laundering. In 2006, following a number of high-level corruption cases, the national strategy was expanded to include anti-corruption initiatives as well.

In 2003, the GOB created specialized money laundering courts. Fifteen of these courts have been established in 14 states, including two in Sao Paulo, with each court headed by a judge who receives specialized training in national money laundering legislation. A 2006 national anti-money laundering strategy goal aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. During November 2007, two judges, a prosecutor and investigator visited the United States as part of an International Visitor Leadership Program to gain information on the U.S. regime for combating money laundering.

Brazil has a limited ability to employ advanced law enforcement techniques such as undercover operations, controlled delivery, and the use of electronic evidence and task force investigations that are critical to the successful investigation of complex crimes, such as money laundering. Generally, such techniques can be used only for information purposes, and are not admissible in court. In 2007, the Ministry of Justice, working through its National Program of Citizens' Public Security (PRONASCI), entered into agreements to establish money laundering forensic laboratories in the Federal District and the states of Rio de Janeiro and Sao Paulo as part of an overall plan to establish ten such facilities in states throughout the country by the end of 2008.

GOB reports appeared to indicate a reversal in 2007 of the upward trend, begun in 2003, of annual growth in the number of money laundering investigations, trials, and convictions. However, the Ministry of Justice indicated that it changed its methodology in 2007 for calculating these statistics to more accurately reflect the number of investigations, trials, and convictions. The Ministry of Justice is currently working to convert data from previous years to correspond to this new methodology, which it expects will lower results from past years. In 2007, there were 590 investigations, 37 trials, and 190 convictions.

Brazil has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets. The COAF and the Ministry of Justice manage these systems jointly. Police authorities and the customs and revenue services are responsible for tracing and seizing assets, and have adequate

police powers and resources to perform such activities. A GOB computerized registry of all seized assets to improve tracking and disbursal is currently being tested and is now in the pilot phase. The judicial system has the authority to forfeit seized assets, and Brazilian law permits the sharing of forfeited assets with other countries.

A COAF-supported amendment, PLS 209, to Law 9.613 was introduced to the legislature in 2003. The bill has passed in the Chamber of Deputies, and is currently in the Senate for consideration. COAF expects the amendment to pass in 2008. If passed, PLS 209 would expand the definition of money laundering to encompass additional predicate offenses, such as tax evasion and trafficking in persons. It would also expand the scope of Law 9.613 to cover games of chance, slot machines and the clandestine art trade; tighten bank secrecy rules; and enhance cooperation between the public prosecutor's office and the COAF. A Senate-proposed amendment to PLS 209 would include penalties for those who finance or collect funds for the purpose of causing crimes that result in widespread panic or constrain the state. The Senate amendments would also require the financial sector to adopt stricter anti-money laundering controls, require attorneys and accountants to report suspicious transactions, and increase the maximum penalty for involvement in money laundering activities from ten to 18 years imprisonment.

Although terrorist financing is considered to be a predicate offense for money laundering under Law 10.701 of 2003, terrorist financing is not an autonomous crime. There have been no money laundering prosecutions to date in which terrorist financing was a predicate offense, and so it remains to be seen if the financing of terrorism could be contested as an enforceable predicate offense due to the lack of legislation specifically criminalizing it. If the Senate-proposed amendment to PLS 209 is adopted, its passage should bring the GOB into greater compliance with the anti-money laundering and counter-terrorist financing standards of the Financial Action Task Force (FATF) and the Egmont Group of financial intelligence units.

The GOB has generally responded to U.S. efforts to identify and block terrorist-related funds. Since September 11, 2001, the COAF has run inquiries on hundreds of individuals and entities, and has searched its financial records for entities and individuals on the UNSCR Sanctions Committee's consolidated list. None of the individuals and entities on the consolidated list has been found to be operating or executing financial transactions in Brazil, and the GOB insists there is no evidence of terrorist financing in Brazil.

On December 6, 2006, the U.S. Department of Treasury placed nine individuals and two entities in the Tri-Border Area that have provided financial or logistical support to Hezbollah on its list of Specially Designated Nationals. The nine individuals operate in the Tri-Border Area and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hezbollah leadership. The two entities, Galeria Page and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used to generate or move terrorist funds. The GOB has publicly disagreed with the designations, stating that the United States has not provided any new information that would prove terrorist financing activity is occurring in the Tri-Border Area.

In 2001, the Mutual Legal Assistance Treaty between Brazil and the Government of the United States (USG) entered into force, and a bilateral Customs Mutual Assistance Agreement, which was signed in 2002, entered into force in 2005. Using the Customs Agreement framework, the GOB's tax and customs authority (Receita Federal) and U.S. Immigration and Customs Enforcement (ICE) established a trade transparency unit (TTU) in 2006 to detect trade-based money laundering. In 2007, Receita conducted five investigations with other law enforcement agencies, resulting in 108 arrests and 5 convictions. ICE and the Brazilian Federal Police currently have two major on-going investigations into trade-based money laundering activities. Future plans include an upgrade of USG and GOB program-related computer systems and USG-sponsored training for Receita officials.

Brazil is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism. Brazil is a member of the FATF and the Financial Action Task Force for South America (GAFISUD). The GOB will hold the presidency of the Financial Action Task Force (FATF) in 2008, and the COAF's director will assume the role of FATF president. Brazil is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The COAF has been a member of the Egmont Group since 1999. The GOB also participates in the "3 Plus 1" Security Group between the United States and the Tri-Border Area countries.

The Government of Brazil should criminalize terrorist financing as an autonomous offense. To continue to successfully combat money laundering and other financial crimes, Brazil should also ensure the passage of legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should enact and implement legislation to provide for the effective use of advanced law enforcement techniques, to provide its investigators and prosecutors with more advanced tools to tackle sophisticated organizations that engage in money laundering, financial crimes, and terrorist financing. Brazil should also enforce currency controls and cross-border reporting requirements, particularly in the Tri-Border region. Additionally, the GOB and the COAF should continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws.

British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK). The BVI remains vulnerable to money laundering, primarily due to drug trafficking and its significant offshore financial services industry. As of June 2007, the BVI has approximately nine banks, 2,550 active mutual funds, 19 local insurance companies, 402 captive insurance companies, 208 trust licenses, seven authorized custodians, 18 company management companies, 100 registered agents, 430 limited partnerships, 10,666 local companies, and 802,850 BVI business companies or international business companies (IBCs).

The BVI International Finance Centre (BVI IFC) was created in 2002 under the Ministry of Finance and Economic Development to promote and market the BVI as an offshore financial center. The BVI IFC recently announced a new outreach program that includes "ambassadors" from the public and private sectors. The "ambassadors" include senior executives and officials from the private sector and the government, including regulators. These individuals will promote the BVI's offshore regime at select trade shows, international conferences, media interviews, and networking events.

The International Business Companies Act (IBCA) of 1984 was created to facilitate companies wishing to conduct international transactions from a tax exempt environment. According to the IBCA, IBCs registered in the BVI cannot engage in business with BVI residents, provide registered offices or agent facilities for BVI-incorporated companies, or own an interest in real property located in the BVI (except for office leases). All IBCs must be registered in the BVI by a registered agent; and the IBC or the registered agent must maintain an office in the BVI. The process for registering banks, trust companies, and insurers is governed by legislation that requires detailed documentation, such as a business plan and vetting by the appropriate supervisor within the Financial Services Commission (FSC). Registered agents must verify the identities of their clients.

As a UK overseas territory, the Government of the British Virgin Islands (GOBVI) has to comply with the European Union Code of Conduct on Business Taxation. The code, among other things, requires that local and offshore companies be treated equally for tax purposes. To address this, and to update the BVI companies' legislation, the BVI Business Companies Act (BCA) 2004 came into force in 2005. The BCA superseded the IBCA act in January 2007, and now exclusively regulates all

companies incorporated in the BVI. The BCA retains many of the same requirements of the IBCA including exemption from BVI taxes, privacy of directors and share registries, no director member residency requirements, and no requirement to file accounts or retain visible and tangible evidence of incorporation. The BCA places all companies, offshore and onshore, within a zero tax regime. Companies registered under the IBCA were provided a two-year transition period. During this period, IBCs had the option of re-registering as business companies under the BCA. Any IBC that did not re-register was automatically re-registered as a business company on January 1, 2007.

While the IBCA only permitted the incorporation of companies limited by shares, the BCA offers seven different types of companies: companies limited by shares, which is the most widely used vehicle; companies limited by guarantee authorized to issue shares, which are typically used for structuring transactions by combining equity and guarantee membership; companies limited by guarantee not authorized to issue shares; unlimited companies that are authorized to issue shares; unlimited companies that are not authorized to issue shares; restricted purposes companies, which are used primarily in structured finance and securitization transactions; and segregated portfolio companies, which are presently limited to insurance companies and mutual funds. The BCA permits the use of numbered names for businesses, i.e. BVI Company # (followed by a number). If a company chooses this format, it will also be permitted to have a foreign character name; an English translation of the name is not required. The BVI reports that Asian countries continue to be a high user of BVI companies, and predicts that the use of BVI companies by Asian countries will increase in the future.

The Financial Services Commission (FSC) is the independent regulatory authority responsible for the licensing and supervision of regulated entities, which include banking and fiduciary businesses, investment businesses, insolvency services, accountants, insurance companies, and company management and registration businesses. Money remitters, however, are not subject to licensing or supervision. The FSC is also responsible for on-site inspections of these entities. The FSC instituted a new penalty regime in 2007. The Financial Services (Administrative Penalties) Regulations went into effect in January 2007, and are intended to deter and penalize regulated entities that are found to be noncompliant with BVI regulatory laws. The lowest penalty that may be imposed is \$100 and the highest is \$20,000.

The FSC cooperates with its foreign counterparts and law enforcement agencies. In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between the BVI's regulators and regulators from other countries. In 2007, the FSC published the Handbook on International Cooperation and Information Exchange. The Handbook is publicly available via the FSC's website and explains the statutory mandates and regulations established in the BVI to facilitate and improve international cooperation.

The Proceeds of Criminal Conduct Act 1997 (POCCA) criminalizes money laundering in the BVI. The POCCA establishes all indictable offences except drug trafficking as predicates for money laundering; drug trafficking predicated money laundering is established under similar provisions in the Drug Trafficking Offences Act 1992. The Proceeds of Criminal Conduct (Amendment) Act, 2006 mandates financial institutions and other providers of financial services to report suspected money laundering transactions. The POCCA allows the BVI Court to grant confiscation orders against those convicted of an offense or who have benefited from criminal conduct. Although procedures exist for the freezing and confiscation of assets linked to criminal activity, including money laundering and terrorist financing, the procedures for the forfeiture of assets that are not directly linked to narcotics-related crimes are unclear.

The POCCA mandates the creation of a financial intelligence unit (FIU), the Reporting Authority. The Financial Investigation Agency Act 2003 reorganizes and renames the FIU. The Financial Investigation Agency (FIA) is responsible for the collection, analysis, investigation, and dissemination of financial information. The FIA receives approximately 200 suspicious transaction reports (STRs)

annually. The FIA's staff is comprised of a director, two senior police officers, one senior customs officer, a chief operating officer, and an administrative assistant. A Board is responsible for setting the policy framework under which the FIA operates. The Board members include the Deputy Governor as chairperson, the Attorney General, the Financial Secretary, Managing Director/CEO of the Financial Services Commission, Commissioner of Police, and Comptroller of Customs. The FIA has a memorandum of understanding (MOU) with the FSC to facilitate information exchange between the two agencies. The FIA exchanges information with foreign counterpart FIUs, and does not require an MOU.

In 2007, the FIA Act was amended to redefine the FIA's responsibilities to include investigation and analysis of any offense in relation to money laundering and terrorist financing, although the financing of terrorism is not an offense in the BVI. The amendment gave the FIA authority to receive disclosures of suspected terrorist financing. It also empowered the FIA to investigate matters relating to the breach of any domestic or international sanction prescribed by or under any enactment.

The Joint Anti-Money Laundering Coordinating Committee (JAMLCC) coordinates all anti-money laundering initiatives in BVI. The JAMLCC is a broad-based, multi-disciplinary body comprised of private and public sector representatives. In December 2000, the Anti-Money Laundering Code of Practice of 1999 (AMLCP) entered into force. The AMLCP establishes procedures to identify suspicious transactions and report them to the FIA. Obligated entities are protected from liability for reporting suspicious transactions. The AMLCP also requires covered entities to create a clearly defined reporting chain for employees to follow when reporting suspicious transactions, and to appoint a reporting officer to receive these reports. The reporting officer must conduct an initial inquiry into the suspicious transaction and report it to the authorities, if sufficient suspicion remains. Failure to report could result in criminal liability. The JAMLCC, in conjunction with the FIA, are currently revising anti-money laundering and counter-terrorist financing guidelines.

The United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 extend to the BVI. The Afghanistan (United Nations Sanctions) (Overseas Territories) Order 2001 and the Al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 also apply to the BVI. However, the BVI has not specifically criminalized the financing of terrorism.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF) and will undergo a mutual evaluation in 2008. The BVI is an Observer to the Offshore Group of Supervisors. The FIA is a member of the Egmont Group, and participates in the Egmont Training Working Group. The BVI is subject to the 1988 UN Drug Convention and, as a British Overseas Territory, has implemented measures in accordance with this convention and the UN Convention against Transnational Organized Crime. The UK extended the application of the UN Convention against Corruption to the BVI in October 2006. Application of the U.S.-UK Mutual Legal Assistance Treaty (MLAT) concerning the Cayman Islands was extended to the BVI in 1990. If an MLAT request's subject matter falls within the FIA's purview, it is forwarded to the FIA for further investigation after it is received and reviewed by the Office of the Attorney General.

The Government of the British Virgin Islands should criminalize the financing of terrorism. The GOBVI should continue to strengthen its anti-money laundering regime by fully implementing its programs and legislation. The BVI should also extend the provisions of its anti-money laundering and counter-terrorist financing regulations to a wider range of entities, including money remitters. The GOBVI should ensure that there are a sufficient number of regulators and examiners to exercise effective due diligence and regulation of its more than 800,000 offshore entities in a manner compliant with international standards.

Bulgaria

Bulgaria is not considered an important regional financial center or an offshore financial center. Its significance in terms of money laundering stems from its geographical position, its well-developed financial sector relative to other Balkan countries, and its relatively lax regulatory control. Although Bulgaria is a major transit point for drugs into Western Europe, it is unknown whether drug trafficking constitutes the primary generator of criminal proceeds and subsequent money laundering in Bulgaria. Financial crimes, including fraud schemes of all types, smuggling of persons and commodities, and other organized crime offenses also generate significant proceeds susceptible to money laundering. Although Bulgaria is primarily a cash economy, ATM and credit card fraud remain serious problems. Tax fraud is prevalent. The sources for money laundered in Bulgaria likely derive from both domestic and international criminal activity. In some cases, organized crime groups, which in the past have operated openly in Bulgaria, are moving into legitimate business operations or even slowly legitimizing themselves, making it difficult to trace the origins of their wealth. Public officials, watchdog institutions, and journalists who challenge organized crime operations often feel intimidated. Smuggling remains a problem in Bulgaria, sustained by ties with shady financiers and corrupt businessmen. While counterfeiting of currency, negotiable instruments, and identity documents has historically been a serious problem in Bulgaria, joint activities by the Government of Bulgaria (GOB) and the U.S. Secret Service have contributed to a decline in counterfeiting in recent years. There has been no indication that Bulgarian financial institutions engage in narcotics-related currency transactions involving significant amounts of U.S. currency or otherwise affecting the United States.

With support and pressure from the United States, the European Union (EU), and nongovernmental organizations (NGOs), the government has continued efforts to address the operation of duty free shops and petrol stations as a funding source for the gray economy and as a conduit for the smuggling of excise goods. Duty free shops play a major role in cigarette smuggling in Bulgaria, as well as smuggling of alcohol, and to a lesser extent perfume and other luxury goods. Attempts by the Ministry of Finance (MOF) to close down all duty free shops and petrol stations operating in Bulgaria have been unsuccessful, in large part due to political opposition within the ruling coalition. Bulgaria's January 2007 accession to the EU mandated the country close nine duty free shops and six petrol stations operating at Bulgaria's borders with neighboring EU countries. However, in December 2006, the Bulgarian Parliament granted permanent licenses for duty free trade to all existing operators and allowed them to relocate businesses to Bulgaria's external nonEU borders. A substantial portion of excise goods sold at duty-free shops and stations stay within the country avoiding taxation. Analysts describe this scheme as protected smuggling, which results in significant losses for the state budget.

While duty free shops and petrol stations are largely perceived as tools to violate customs and tax regimes, duty free shops may be used to facilitate other crimes, including financial crimes. Credible allegations have linked duty free trade in Bulgaria to organized crime interests involved in fuel smuggling, forced prostitution, the illicit drug trade, and human trafficking. There is no indication, of links between duty free shops or free trade areas and terrorist financing. The MOF's Customs Agency and General Tax Directorate have supervisory authority over the duty free shops. According to some NGOs, reported revenues and expenses by the shops have clearly included unlawful activities, in addition to duty free trade. Good procedures for identifying unlawful activity are lacking. MOF inspections have revealed that it is practically impossible to monitor whether customers at the numerous duty free shops have actually crossed an international border.

Article 253 of the Bulgarian Penal Code criminalizes money laundering. Amendments made to the Penal Code in 2006 increase penalties (including in cases of conspiracy and abuse of office), clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in Bulgaria, and allow prosecution on money laundering charges without first obtaining a conviction for

the predicate crime. Article 253 criminalizes money laundering related to all crimes. As such, drug trafficking is but one of many recognized predicate offenses.

The Law on Measures against Money Laundering (LMML) is the legislative backbone of Bulgaria's anti-money laundering regime. The LMML was adopted in 1998 and has since been amended several times, most recently in 2007. Bulgaria has strict and wide-ranging banking, tax, and commercial secrecy laws that limit the dissemination of financial information absent the issuance of a court order. Bulgaria's financial intelligence unit (FIU), the Financial Intelligence Agency (FIA), is the main administrative unit for collecting and analyzing information on suspected money laundering transactions. Unlike all other government institutions, the FIU is not bound by the typical secrecy provisions that are often cited as an impediment to law enforcement functions. In an effort to lessen the impact of secrecy laws on law enforcement functions, in 2006, the GOB issued amendments to both the LMML and the Law on Credit Institutions. The amendments to the Law on Credit Institutions facilitate the investigation and prosecution of financial crimes by giving the Prosecutor General the right to request financial information from banks without a court order in cases involving money laundering and organized crime. The FIA does not participate in criminal investigations.

Prior to December 2007, the FIA was a fully independent agency operating under the MOF, with the independence of the FIA director being guaranteed by the LMML. It had the authority to perform onsite compliance inspections, obtain information without a court order, share all information with law enforcement, and receive reports of suspected terrorist financing. However, on December 11, 2007, the Parliament passed legislation, which came into force on January 1, 2008. This law, the Act on the State Agency for National Security, established a new national intelligence agency, the State Agency for National Security (SANS). The law also restructures the FIA by changing its status from an independent agency within the MOF to a directorate within the SANS. The legislation lacks clarity regarding the new FIU's autonomy, operational status, and ability to exchange information consistent with international standards. The FIU's ability to conduct on-site inspections as well as its free access all government databases has been removed. In addition, the analytical capacity of FIA is not precisely defined: the SANS law permits the FIU to acquire and handle national security-related information, but financial crimes information is not necessarily of national security importance. The FIA is no longer an individual legal entity with its own budget. The status of the joint instructions signed between FIA and other government organizations such as the Ministry of Interior and the Prosecution Service is now unclear. The FIA's authority to exchange information with international partners, which was explicitly provided for in the LMML, has been removed. Exchange of classified information with other Bulgarian agencies is not clearly defined.

Although the oversight and other authorities of the new FIU are set to be addressed in supplemental legislation or implementing regulations that are to be drafted by March 2008, each of the legal gaps listed above potentially undermines the financial intelligence unit's ability to execute its mission and uphold its international commitments. As such, in January 2008, the Egmont Group temporarily suspended Bulgaria's access to their secure information exchange system, pending further clarification of the FIU's proposed structure and operational capacities.

Banks and the 29 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. Since 2003, all reporting entities are required to ask for the source of funds in any transaction greater than 30,000 BGN (approximately \$22,500) or foreign exchange transactions greater than 10,000 BGN (approximately \$7,500). Reporting entities are also required to notify the FIA of any cash payment greater than 30,000 BGN (\$22,500). Current reporting requirements do not mandate that banks and other reporting entities report the actual amounts involved in a currency transaction greater than 30,000 BGN (\$22,500); they are only required to report the fact that such a transaction occurred. Concerted action by NGOs and others is underway to convince the MOF and the Bulgarian National Bank (BNB) to change the law so as to require reporting of the actual amount of the transaction.

The LMML obligates financial institutions to a five-year record keeping requirement and provides a “safe harbor” to reporting entities. Penal Code Article 253B was enacted in 2004 to establish criminal liability for noncompliance with LMML requirements. Although case law remains weak, Bulgaria’s anti-money laundering legislation was determined to be in full compliance with all EU standards when it was assessed in September 2003 for purposes of EU accession.

In 2006, the Ministry of the Interior (MOI), the Prosecutor’s Office, and the FIA signed a joint instruction establishing new procedures for closer cooperation when following leads contained in a suspicious transaction report (STR). A 2007 supplement to the instruction institutes a political-level contact group comprised of high-level representatives of the three institutions to improve cooperation. As of October 2007, the group had held two meetings to discuss cooperation mechanisms and improved protection of the reporting entities’ employees. Reports prepared by FIA were forwarded to the Prosecutor General with a copy for the MOI, which subsequently produced a report on the enforcement potential of the case within 30 days of receipt.

From January 2007 through October 2007, the FIA received 293 STRs on money laundering, totaling 219,291,944 BGN (approximately \$161,244,000). The FIA also received one STR on suspected terrorist financing activity. During the same period, the FIA received 158,000 currency transaction reports (CTRs). On the basis of the forwarded reports, 249 cases valued at 219,191,944 BGN (approximately \$161,170,000) were opened, 15 cases valued at 35,309,072 BGN (approximately \$26,000,000) were referred to the Supreme Prosecutor’s Office of Cassation, and 203 cases valued at 151,337,126 BGN (approximately \$111,278,000) were referred to the Ministry of Interior and copied to the Supreme Cassation Prosecution.

In response to pressure from the EU, in 2006, Bulgaria’s Parliament tightened the LMML with further amendments. These amendments expanded the definition of money laundering and the list of reporting entities; outlawed anonymous bank accounts; expanded the definition of “currency”; and required the disclosure of source for currency exported from the country. Under the LMML, 30 categories of entities, including lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators, are required to file suspicious transactions reports. The banking sector has substantially complied with the law’s filing requirement. Reporting by other sectors, however, has been much lower. Historic lower rates of reporting compliance by exchange bureaus, casinos, and other nonbank financial institutions can be attributed to numerous factors, including a lack of understanding of or respect for legal requirements, lack of inspection resources, and the general absence of effective regulatory control over the nonbank financial sector.

Following the 2006 amendments to the LMML, which instituted compliance checks for the nonbanking sector, the FIA noted a slight improvement in reporting. As of October 2007, the FIA inspected four banks, 19 exchange offices, 14 financial houses, three insurance companies, eight investment intermediaries, four casinos, 10 public notaries, four leasing undertakings, six car dealers, five sports organizations, one wholesale dealer, and eight real estate agents in 2007, imposing fines in 42 cases. Most of the violations disclosed were for failure to declare the origin of funds, perform identification procedures for clients, or report transactions over 30,000 BGN (approximately \$22,500). The National Revenue Agency also conducted 509 on-site inspections of exchange offices.

In October 2006, the courts rendered the country’s first two convictions for money laundering. In 2007, money laundering convictions increased, reaching 11 by October. A total of 25 people were indicted on money laundering charges. Only four of the initiated cases ended in acquittal and nine were awaiting a court’s decision.

Although there are few indications of terrorist financing directly connected with Bulgaria, the possibility remains that terrorism-related funds can transit across Bulgarian borders through cash couriers and other informal mechanisms. Article 108a of the Penal Code criminalizes terrorism and terrorist financing. Article 253 of the Criminal Code qualifies terrorist acts and terrorist financing as

predicate crimes under the “all crimes” approach to money laundering. In February 2003, the GOB enacted the Law on Measures Against Terrorist Financing (LMATF), which links counterterrorism measures with financial intelligence, and compels all covered entities to report any suspicion of terrorist financing or pay a penalty of up to 50,000 BGN (approximately \$37,500). The law is consistent with Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing, and authorizes the FIA to use its resources and financial intelligence to combat terrorist financing along with money laundering.

Under the LMATF, the GOB may freeze the assets of a suspected terrorist for 45 days. Key players in the process of asset freezing and seizing, as prescribed in existing law, include the MOI, MOF (including the FIA), Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General. The FIA and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations, as found on the UNSCR 1267 Sanctions Committee’s Consolidated List, as well as the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224, and those designated by the relevant EU authorities. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities.

Although alternative remittance systems may operate in Bulgaria, their scope is unknown and there are no reported initiatives underway to address them. In general, regulatory controls over nonbank financial institutions are weak, with some of those institutions engaging in banking activities absent any regulatory oversight. Some anecdotal evidence suggests that charitable and nonprofit legal status is occasionally used to conceal money laundering.

The Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Both the money laundering and the terrorist financing laws include provisions for identifying, tracing, and freezing assets related to money laundering or the financing of terrorism. A new criminal asset forfeiture law, targeted at confiscation of illegally acquired property, came into effect in March 2005. The law permits forfeiture proceedings to be initiated against property valued in excess of 60,000 BGN (approximately \$45,100) if the owner of the property is the subject of criminal prosecution for enumerated crimes (terrorism, drug trafficking, human trafficking, money laundering, bribery, major tax fraud, and organizing, leading, or participating in a criminal group) and a reasonable assumption can be made that the property was acquired through criminal activity. As required by the law, an Assets Identification Commission was established and became operational in 2006. The Commission has the authority to institute criminal asset identification procedures, as well as request from the court both preliminary injunctions and ultimately the forfeiture of assets. As of March 2007, the Commission has filed with the court 38 injunction requests for property valued at 19,037,365 BGN (approximately \$14.2 million) and 10 forfeiture requests for property valued at 3,453,783 BGN (approximately \$2.5 million).

In September 2007, the United States and Bulgaria signed a mutual legal assistance treaty (MLAT), implementing the U.S.-EU Mutual Legal Assistance Agreement, which has yet to come into force. The 2005 ratification of the UN Convention against Transnational Organized Crime by the U.S. established an MLAT-type relationship between the two countries (Bulgaria having ratified the Convention in 2001). As of October 2007, the FIA had bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 28 countries. The FIA is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. As of October 2007, the FIA sent 261 requests for information to foreign FIUs and received 54 requests for assistance from foreign FIUs.

Bulgaria participates in the Council of Europe’s Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The most recent mutual evaluation of Bulgaria was conducted by MONEYVAL in 2007. The mutual evaluation report (MER) is still in draft format.

The FIA is a member of the Egmont Group and also participates in information sharing with foreign counterparts. As of January 1, 2008, some of the FIA's rights within the Egmont Group were temporarily suspended pending a review of its authorities under the new legislation for the State Agency for National Security. Bulgaria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. The GOB is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

In 2005, the Bulgarian Parliament passed amendments to the 1969 law on Administrative Violations and Penalties, which establishes the liability of legal persons (companies) for crimes committed by their employees. This measure is in accordance with international standards and allows the government to implement its obligations under international agreements, including: the OECD Anti-Bribery Convention, the Civil Law Convention on Corruption, the Criminal Law Convention on Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Under the amendments, Bulgaria also aligns itself with the provisions of the EU Convention on the Protection of the Financial Interests of the European Communities and its Protocols.

Until December 2007 Bulgaria's legislative framework was largely viewed as consistent with international anti-money laundering standards. The new legislation on the State Agency for National Security brings uncertainty as to the authority of the financial intelligence unit, potentially jeopardizing its independence and investigatory mandate. It also raises questions about the FIA's ability to cooperate on equal basis with its international partners. The Government of Bulgaria should address these issues. The GOB should also take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors and cash payments. The GOB should improve the consistency of its customs reporting enforcement and should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. Inter-agency cooperation should be streamlined to ensure effective implementation of Bulgaria's anti-money laundering and counter-terrorist financing regime, and to improve prosecutorial effectiveness in money laundering and terrorist financing cases. The GOB should close duty free shops, or establish procedures for identifying unlawful activities associated with duty free shops, thereby tackling organized crime involved in smuggling and other financial crimes. The GOB should also disseminate the UNSCR 1267 Sanctions Committee's Consolidated List of designated terrorist entities to all financial institutions.

Burma

Burma, a major drug-producing country, has taken steps to strengthen its anti-money laundering regulatory regime in 2007. The country's economy remains dominated by state-owned entities, including the military. Agriculture and extractive industries, including natural gas, mining, logging and fishing provide the major portion of national income, with heavy industry and manufacturing playing minor roles. The steps Burma has taken over the past several years have reduced vulnerability to drug money laundering in the banking sector. However, with an underdeveloped financial sector and large volume of informal trade, Burma remains a country where there is significant risk of drug money being funneled into commercial enterprises and infrastructure investment. Traffic in narcotics, people, wildlife, gems, timber, and other contraband flow through Burma. Regionally, value transfer via trade is of concern and hawala/hundi networks frequently use trade goods to provide counter-valuation. Burma's border regions are difficult to control and poorly patrolled. In some remote regions active in smuggling, there are continuing ethnic tensions with armed rebel groups that hamper government control. Collusion between traffickers and Burma's ruling military junta, the State Peace and Development Council (SPDC), allows organized crime groups to function with virtual impunity.

Although progress was made in 2007, the criminal underground faces little risk of enforcement and prosecution. Corruption in business and government is a major problem. Burma is ranked 179 out of 179 countries in Transparency International's 2007 Corruption Perception Index.

The Government of Burma (GOB) has addressed some key areas of concern identified by the international community by implementing some anti-money laundering measures. In October 2006, the Financial Action Task Force (FATF) removed Burma from the FATF list of Non-Cooperative Countries and Territories (NCCT). To ensure continued effective implementation of reforms in Burma, the FATF, in consultation with the relevant FATF-style regional body (FSRB), will continue to monitor developments there for a period of time after de-listing. Burma is scheduled to undergo a mutual evaluation by the FSRB Asia-Pacific Group on Money Laundering in January 2008.

The United States maintains other sanctions on trade, investment and financial transactions with Burma under Executive Order 13047 (May 1997), Executive Order 13310 (July 2003), the Narcotics Control Trade Act, the Foreign Assistance Act, the International Financial Institutions Act, the Export-Import Bank Act, the Export Administration Act, the Customs and Trade Act, the Tariff Act (19 USC 1307), and the 2003 Burmese Freedom and Democracy Act (P.L. 108-61). In September and October 2007, under Executive Order 13310, the United States imposed additional sanctions on leaders of the Burmese regime, as well as key businessmen. In October 2007, Executive Order 13448 was issued. It expands the Treasury Department's existing authority to designate individuals for sanctions to include individuals responsible for human rights abuses and public corruption and individuals and entities who provide material or financial support to designated individuals or to the Government of Burma.

Burma enacted a "Control of Money Laundering Law" in 2002. It also established the Central Control Board of Money Laundering in 2002 and a financial intelligence unit (FIU) in 2003. The law created reporting requirements to detect suspicious transactions. It set a threshold amount for reporting cash transactions by banks and real estate firms, albeit at a high level of 100 million kyat (approximately U.S. \$75,000). As of May 2007, over 40,000 cash transaction reports were filed. The GOB's 2004 anti-money laundering measures amended regulations instituted in 2002-2003 that set out 11 predicate offenses, including narcotics activities, human trafficking, arms trafficking, cyber-crime, and "offenses committed by acts of terrorism," among others. In 2004 the GOB added fraud to the list of predicate offenses, established legal penalties for leaking information about suspicious transaction reports, and adopted a "Mutual Assistance in Criminal Matters Law." The 2003 regulations, further expanded in 2006, require banks, customs officials and the legal and real estate sectors to file suspicious transaction reports (STRs) and impose severe penalties for noncompliance.

The GOB established a Department against Transnational Crime in 2004. Its mandate includes anti-money laundering activities. It is staffed by police officers and support personnel from banks, customs, budget, and other relevant government departments. In response to a February 2005 FATF request, the GOB submitted an anti-money laundering implementation plan and produced regular progress reports in 2006 and 2007. In 2005, the government also increased the size of the FIU to 11 permanent members, plus 20 support staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports that review banks' compliance with AML legislation. Since then, the Central Bank has sent teams to instruct bank staff on the new guidelines and to inspect banking operations for compliance.

In 2007, the Burmese Government amended its "Control of Money Laundering Law" to expand the list of predicate offenses to all serious crimes to comport with FATF's recommendations. In July 2007, the Central Control Board issued five directives to bring more nonbank financial institutions, including dealers in precious metals and stones, under the AML/CTF compliance regime. As of August 2007, 823 STRs had been received. One case related to trafficking in persons was filed for prosecution, resulting in the convictions of one individual under the "Control of Money Laundering

Law” and the Trafficking in Persons Law. In the first eight months of 2007, seven cases have been identified as potential money laundering investigations.

The United States maintains the separate countermeasures it adopted against Burma in 2004, and identified the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be “of primary money laundering concern” pursuant to Section 311 of the 2001 USA PATRIOT Act. These countermeasures prohibited U.S. banks from establishing or maintaining correspondent or payable-through accounts in the United States for or on behalf of Myanmar Mayflower and Asia Wealth Bank and, with narrow exceptions, for all other Burmese banks. Myanmar Mayflower and Asia Wealth Bank had been linked directly to narcotics trafficking organizations in Southeast Asia. In March 2005, following GOB investigations, the Central Bank of Myanmar revoked the operating licenses of Myanmar Mayflower Bank and Asia Wealth Bank, citing infractions of the Financial Institutions of Myanmar Law. The two banks no longer exist. In August 2005, the Government of Burma also revoked the license of Myanmar Universal Bank (MUB), and convicted the bank’s chairman under both the Narcotics and Psychotropic Substances Law, and the Control of Money Laundering Law. Under the money laundering charge, the court sentenced him to one 10-year and one unlimited term in prison and seized his and his bank’s assets.

Burma also remains under a separate 2002 U.S. Treasury Department advisory stating that U.S. financial institutions should give enhanced scrutiny to all financial transactions related to Burma. The Section 311 rules complement the 2003 Burmese Freedom and Democracy Act (renewed in July 2006) and Executive Order 13310 (July 2003), which impose additional economic sanctions on Burma following the regime’s May 2003 attack on a peaceful convoy of the country’s pro-democracy opposition led by Nobel laureate Aung San Suu Kyi. The sanctions prohibit the import of most Burmese-produced goods into the United States, ban the provision of financial services to Burma by any U.S. persons, freeze assets of the ruling junta and other Burmese institutions, and expand U.S. visa restrictions to include managers of state-owned enterprises as well as senior government officials and family members associated with the regime. In September 2007, the U.S. Treasury amended and reissued the Burmese Sanctions Regulations in their entirety to implement the 2003 Executive Order that placed these sanctions on Burma.

Burma became a member of the Asia/Pacific Group on Money Laundering in March 2006. The GOB is a party to the 1988 UN Drug Convention. Over the past several years, Burma has expanded its counter narcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand. These agreements include cooperation on drug-related money laundering issues. In July 2005, the Myanmar Central Control Board signed an MOU with Thailand’s Anti-Money Laundering Office governing the exchange of information and financial intelligence. The government signed a cooperative MOU with Indonesia’s FIU in November 2006.

Burma is a party to the UN Convention against Transnational Organized Crime and ratified the UN International Convention for the Suppression of the Financing of Terrorism in August 2006. Burma signed the UN Convention on Corruption in December 2005, but has yet to deposit an instrument of ratification with the UN Secretary General. Likewise, Burma signed the Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries in January 2006, but has yet to deposit its instrument of ratification with the Attorney General of Malaysia.

The Government of Burma has in place a framework to allow mutual legal assistance and cooperation with overseas jurisdictions in the investigation and prosecution of serious crimes. To fully implement a strong anti-money laundering/counter-terrorist financing regime, Burma must provide the necessary resources to administrative and judicial authorities who supervise the financial sector so they can apply and enforce the government’s regulations to fight money laundering successfully. Burma must also continue to improve its enforcement of the new regulations and oversight of its banking system,

and end all government policies that facilitate the investment of drug money and proceeds from other crimes into the legitimate economy. The reporting threshold for cash transactions should be lowered to a realistic threshold that fits the Burmese context. Customs should be strengthened and authorities should monitor more carefully the misuse of trade and its role in informal remittance or hawala/hundi networks. The GOB should ratify the UN Convention against Corruption, as well as the Treaty On Mutual Legal Assistance In Criminal Matters Among Like-Minded ASEAN Member Countries. The GOB should take serious steps to combat smuggling of contraband and its link to the pervasive corruption that permeates all levels of business and government. The GOB should criminalize the financing of terrorism.

Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. While there are only four reported money laundering cases in Cambodia, it serves as a transit route for heroin from Burma and Laos to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. The major crimes reported by the Cambodian authorities are human trafficking and exploitation (which is widespread), drug trafficking, kidnapping for ransom and corruption. Its weak but improving anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling and widespread corruption of officials also contributes to the significant money laundering risk in Cambodia. The vulnerability of Cambodia's financial sector is further exacerbated because of the intersection of the casino and banking interests with four companies having whole or partial shares in both banks and casinos. In addition, terrorist financing is a significant risk in Cambodia as highlighted by two recent cases involving Jemaah Islamiyah (JI) and the Cambodian Freedom Fighters (CFF).

In June 2007, The Royal Government of Cambodia promulgated a new "Law on Anti-Money Laundering and Combating the Financing of Terrorism" (AML). This law creates the framework for a National Bank of Cambodia financial investigations unit (FIU) to have far-reaching regulation over all banks and a long list of nonbank financial institutions such as casinos and realtors and can include entities to be designated by the FIU. In July 2007, a new Counterterrorism Law criminalized the financing and provision of material support to terrorism.

The National Bank of Cambodia (NBC) is making strides to regulate large or suspicious financial transactions, but is still in the process of working with relevant ministries to draft a prakas (decree) and related sub-decrees to fully implement the new anti-money laundering law. The prakas is expected to be issued in the first half of 2008. The Ministry of Interior has legal responsibility for oversight of the casinos and providing security; however, it exerts little supervision.

Cambodia's banking sector is small but expanding, with fifteen commercial banks, five specialized banks, and numerous microfinance institutions. Bank operations are primarily undertaken in U.S. dollars and on a cash basis. However, overall lending and banking activity remains limited as most Cambodians keep their assets outside the banking system. Economists note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 29.2 percent (September 2007), low even by developing economy standards. Cambodia's banking system is highly consolidated, with two banks—Canadia Bank and ANZ Royal—accounting for more than 30 percent of all bank deposits. Besides banks, individual and legal persons can undertake foreign exchange provided they register with the NBC. There were 647 registered money changers in December 2006—53 in Phnom Penh and 594 in provinces.

The NBC has regulatory responsibility for the banking sector. The NBC regularly audits individual banks to ensure compliance with laws and regulations. The new AML law requires that banks and other financial institutions declare transactions over 40,000,000 riel (approximately U.S. \$10,000). The NBC reports that its audits reveal that this requirement is generally followed. While there are no

reports to indicate that banking institutions themselves are knowingly engaged in money laundering, until the FIU is fully established, government audits would likely not be a sufficient deterrent to money laundering through most Cambodian banks. With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have risen by about 15 percent per year since 2000 and the financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Foreign direct investment, while limited, is increasing after several years of contraction.

Cambodia lacks meaningful statistics on the extent of financial crime which exists and only a few crime statistics and open source information is available to evaluate the major sources of illicit funds in Cambodia. As the FIU is still being established, some larger scale money laundering in Cambodia may also flow through informal banking activities or business activities. The Cambodian authorities consider that there are informal money or value transfer operations carried out by money changers, or individuals within Cambodia or cross border. There is a significant black market in Cambodia for smuggled goods, including drugs, including the importing and local production of the methamphetamine ATS. Most of the smuggling that takes place is intended to circumvent official duties and taxes and involves items such as fuel, alcohol and cigarettes. Some government officials and their private sector associates have a significant amount of control over the smuggling trade and its proceeds. Cambodia has a cash-based and dollar-based economy, and the smuggling trade is usually conducted in dollars. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily converted into land, housing, luxury goods or other forms of property. It is also relatively easy to hand-carry cash into and out of Cambodia.

The NBC's Financial Investigations Unit (FIU) has the authority to apply anti-money laundering controls to nonbank financial institutions such as casinos and other intermediaries, such as lawyers or accountants. The FIU is under the control of the NBC with a permanent secretariat working under the authority of a board composed of one senior representative each from the Council of Ministers and the Ministries of Economy and Finance, Justice, and Interior.

The major nonbank financial institutions in Cambodia are the casinos, which the authorities have noted are particularly vulnerable to money laundering. Foreigners are allowed to gamble but Cambodians nationals are prohibited from entering casinos. The regulation of casinos falls under the jurisdiction of the Ministry of Interior, although the Ministry of Economy and Finance issues casino licenses and the NBC Financial Investigations Unit will have the newly legislated power to receive reports on financial transactions at casinos and cooperate with casino regulators on AML, including suspicious transactions. There are currently more than 20 licensed casinos in Cambodia, with a few more either under construction or applying for a license. Most are located along Cambodia's borders with Thailand or Vietnam. There is one large casino in Phnom Penh that has avoided the regulation that all casinos be at least 200 kilometers from the capital city. Casino patrons placing small bets simply hand-carry their money across borders, while others use either bank transfers or junket operators. Cambodian casinos have accounts with major Thai or Vietnamese banks and patrons can wire large amounts of money to one of these foreign accounts. After a quick phone call to verify the transfer, the Cambodian casino issues the appropriate amount in chips. Casinos also work with junket operators who, despite their name, only facilitate money transfers and do not serve as travel or tour operators. Players deposit money with a junket operator in Vietnam or Thailand, the casino verifies the deposit and issues chips to the player-typically up to double the amount of the deposit. After the gambling session ends, the junket operator then has 15 days to pay the casino for any losses. Because the junket operator is responsible for collecting from the patrons, casinos see little need to investigate the patron's ability to cover his/her potential debt or the source of his/her wealth.

Although there is a legal requirement to declare to Cambodian Customs the entry of more than U.S. \$10,000 into the country, in practice there is no effective oversight of cash movement into or out of Cambodia. Article 13(1) of the Law of Foreign Exchange requires the import or export of any means

of payment equal to or exceeding U.S. \$10,000 or equivalent to be reported to the Customs authorities at the border crossing point and Customs should transmit this information on a monthly basis to the National Bank of Cambodia. Outbound travelers are in practice not required to fill in a declaration form concerning the amount of currency or negotiable instruments they are carrying. There is no explicit power to stop or restrain transported funds and negotiable instruments to ascertain whether evidence of money laundering or terrorist financing exists. No specific provisions exist to sanction persons involved in cross border cash smuggling for money laundering or terrorist financing purposes or seize the cash or instruments involved.

In 1996, Cambodia criminalized money laundering related to narcotics trafficking through the Law on Drug Control. In 1999, the government also passed the Law on Banking and Financial Institutions. Together with the recently passed AML law, these two laws provide an additional legal basis for the NBC to regulate the financial sector. The NBC also uses the authority of these laws to issue and enforce new regulations. The NBC expects to issue a prakas (decree) on the AML in the first half of 2008. One current regulation, dated October 21, 2002, is specifically aimed at money laundering. The decree established standardized procedures for the identification of money laundering at banking and financial institutions. In October 2003, the NBC issued a circular to assist banks in identifying suspicious transactions and in fulfilling “Know Your Customer” best practices, though no suspicious transactions have yet been reported to the NBC. In addition to the NBC, the Ministries of Economy and Finance, Interior, Foreign Affairs, and Justice also are involved in anti-money laundering matters.

In 2005, Cambodia became a party to the 1988 UN Drug Convention, the UN Convention Against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. The new Counterterrorism Law criminalizes terrorist financing; and regulation of transactions suspected of financing terrorism are covered by the new AML. Under the new counter terrorism law the Minister of Justice may order the prosecutor to freeze property of a person if he is listed on the list of persons and entities belonging or associated with the Taliban and Al Qaida issued by the UNSCR 1267 committee or if he is a person who has committed an offence as defined in the law or a corresponding offence under the law of another state. The NBC circulates to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee’s consolidated list, and reviews the banks for compliance in maintaining this list and reporting any related activity. To date, there has not been an opportunity to monitor compliance of these new provisions. However, there have been no reports of designated terrorist financiers using the Cambodian banking sector. Should sanctioned individuals or entities be discovered using a financial institution in Cambodia, the NBC has the legal authority to freeze the assets until prosecution commences and a competent court has adjudicated the case. Penal sanctions for convictions of money laundering or financing terrorism include seizure of the assets to become state property.

In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) style regional body. In May 2007, Cambodia underwent a comprehensive AML/CTF assessment that was conducted by the World Bank and APG. This assessment report was adopted by the APG in July 2007 and noted the progress, and remaining deficiencies the GOC’s AML/CTF regime. This report marks the first time there has been detailed external scrutiny of AML/CTF in Cambodia and publication of the findings. However, questions regarding the government’s ability to implement and enforce the new measures on money laundering remain, and approval of an implementing decree and related sub-decrees are important next steps. The GOC should also take the necessary steps to enhance its nascent FIU and should gain control over its porous borders as well as increasing the capability of its law enforcement and judicial sectors to investigate, prosecute and adjudicate financial crimes. To achieve these ends, the GOC should continue its engagement with the Asia/Pacific Group on projects supported by the United States, Australia, the World Bank and the UN Office on Drugs and Crime (UNODC) to develop a comprehensive viable anti-money laundering/counter-terrorist financing regime that comports with international standards.

Canada

Money laundering in Canada is primarily associated with drug trafficking and financial crimes, particularly those related to fraud. The International Monetary Fund indicates that approximately U.S. \$22-50 billion is laundered annually in Canada. Organized criminal groups involved in drug trafficking remain a concern of the Government of Canada (GOC). According to the Criminal Intelligence Service Canada's 2007 Annual Report on Organized Crime, there are approximately 950 organized crime groups operating in Canada, with approximately 80 percent of all crime groups in Canada involved in the illicit drug trade. With U.S. \$1.5 billion in trade crossing the border each day, both the United States and Canadian governments are concerned about the criminal cross-border movements of currency, particularly the illicit proceeds of drug trafficking.

The GOC enacted the Proceeds of Crime (Money Laundering) Act in 2000 to assist in the detection and deterrence of money laundering, facilitate the investigation and prosecution of money laundering, and create the financial intelligence unit (FIU), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The Proceeds of Crime (Money Laundering) Act was amended in December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The list of predicate money laundering offenses was expanded to cover all indictable offenses, including terrorism and the trafficking of persons. In addition to amending the PCMLTFA, the 2001 reforms made it a crime under the Canadian Criminal Code to knowingly collect or give funds to carry out terrorism; denied or removed charitable status from those supporting terrorism; and facilitated freezing and seizing their assets.

The PCMLTFA created a mandatory reporting system for suspected terrorist property, suspicious financial transactions, large cash transactions, large international electronic funds transfers, and cross-border movements of currency and monetary instruments totaling \$10,000 or more. Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from approximately U.S. \$250 to \$5,000. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately U.S. \$2 million, or both. The law protects those filing suspicious transaction reports from civil and criminal prosecution. There has been no apparent decline in deposits made with Canadian financial institutions as a result of Canada's revised laws and regulations.

In December 2006, Parliament passed Bill C-25 to amend the PCMLTFA. The new legislation expands the coverage of Canada's anti-money laundering and counter-terrorist financing regime by bringing additional business sectors, including lawyers and dealers in precious metals and stones, under the authority of the PCMLTFA and related regulations. Bill C-25 also enhances client identification and record-keeping requirements. In addition, Bill C-25 mandates that FINTRAC create a national registry for money service businesses, and establish a system of administrative monetary penalties for noncompliance. The proposed measures will improve compliance with the reporting, record keeping, and client identification provisions of the PCMLTFA. The Bill permits FINTRAC to include additional information in the intelligence product that FINTRAC can disclose to law enforcement and national security agencies, as recommended in a 2004 Canadian Auditor General's Report.

FINTRAC, established in 2006, is an independent agency with regulatory and FIU functions. The majority of FINTRAC's 300-member staff works as analysts, compliance officers, and information technology specialists. FINTRAC is the sole authority with the mandate to ensure compliance with the PCMLTFA and associated regulations. Guidelines explaining the PCMLTFA and its requirements were published by FINTRAC in 2002; further additions were made in 2003 and in July 2007. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing, including their international scope and nature. The guidelines also provide an outline of the Canadian legislative requirements for a

compliance regime, record-keeping, client identification, and reporting transactions. FINTRAC also works closely with Canada's Office of the Superintendent of Financial Institutions (OSFI) concerning the policies and procedures that reporting entities have in place for complying with the PCMLTFA.

FINTRAC's compliance program is risk-based and emphasizes awareness training, compliance examinations, disclosures to law enforcement of reporting entities' noncompliance, and minimizing the regulatory burden for obligated entities. During 2006 and 2007, over 14,000 individuals representing all reporting sectors participated in a variety of FINTRAC's awareness initiatives. FINTRAC has Memoranda of Understanding (MOUs) with Canadian national regulators, including OSFI and the Investment Dealers Association of Canada (IDA), as well as provincial regulators. These MOUs permit FINTRAC and the regulators to exchange compliance information. FINTRAC, together with national and provincial regulators, conducted a record number of compliance examinations across all reporting sectors in 2006 and 2007.

As Canada's FIU, FINTRAC receives and analyzes reports from financial institutions and other financial intermediaries (such as money service businesses, casinos, accountants, and real estate agents) as mandated by the PCMLTFA, and makes disclosures to law enforcement and intelligence agencies. FINTRAC may only disclose information related to money laundering or terrorist financing offences. FINTRAC has access to other law enforcement and national security agencies databases through an MOU and, on a case-by-case basis, with other relevant agencies. FINTRAC received approximately 15 million reports from reporting entities in 2006 and 2007, which includes approximately 29,000 suspicious transaction reports (STRs), 6 million cash transaction reports, 50,000 cross-border reports, and 9 million electronic funds transfer reports (which includes funds that enter and exit the country). FINTRAC produced a total of 193 case disclosures in 2006 and 2007, totaling approximately \$10 billion. Of the 193 case disclosures, 152 were suspected money laundering, 33 were suspected terrorist activity, and 8 involved suspected money laundering, terrorist financing, and/or threats to the security of Canada. FINTRAC has the ability to exchange information with foreign FIUs through an MOU, and has signed over 45 MOUs with its counterparts. In 2006 and 2007, FINTRAC made 35 disclosures to 14 counterpart FIUs.

In a 2004 report to Parliament, Canada's Auditor General stated that "privacy concerns restrict FINTRAC's ability to disclose intelligence to the Police, and as a result, law enforcement and security agencies usually find that the information they receive is too limited to justify launching investigations." United States law enforcement officials have echoed concerns that Canadian privacy laws and the high standard of proof required by Canadian courts inhibit the full sharing of timely and meaningful intelligence on suspicious financial transactions. Such intelligence may be critical to investigating and prosecuting international terrorist financing or major money laundering investigations. Recently, concern has focused on the inability of United States and Canadian law enforcement officers to exchange information promptly concerning suspicious sums of money found in the possession of individuals attempting to cross the United States-Canadian border. A 2005 MOU on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive.

The PCMLTFA enables Canadian authorities to identify, deter, disable, prosecute, convict, and punish terrorist groups. The PCMLTFA expands FINTRAC's mandate to include counter-terrorist financing and allow disclosure to the Canadian Security Intelligence Service of information related to financial transactions relevant to threats to the security of Canada. The GOC has also listed and searched financial records for suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. This designation effectively freezes their assets and prohibits fund-raising on their behalf in Canada.

In addition to new legislation, the GOC is undertaking other initiatives to bolster its ability to combat money laundering and terrorist financing. Canada's Department of Finance has created a public/private sector advisory committee to discuss matters of mutual interest in the ongoing fight against money laundering and counter-terrorist financing. In May 2006, the GOC announced that it had added in the 2006 budget approximately U.S. \$58 million over the next two years for FINTRAC, the Royal Canadian Mounted Police (RCMP), and the Department of Justice. The new funding will increase the number of RCMP officers working in the counter-terrorist financing and anti-money laundering units; increase the capabilities of the Canada Border Services Agency (CBSA) to detect unreported currency at airports and border crossings; enable Canada's Department of Justice to handle the expanding litigation workload that will result from increasing the enforcement resources of other GOC agencies; and ensure that FINTRAC can better analyze transactions reports and monitor compliance of unregulated financial sectors, such as money remitters.

Canada has longstanding agreements with the United States on law enforcement cooperation, including treaties on extradition and mutual legal assistance, as well as an asset sharing agreement. Canada has provisions for sharing seized assets, and exercises them regularly. The CBSA and the United States Department of Homeland Security Immigration and Customs Enforcement (ICE) are in the process of negotiating an MOU to share information on currency seizures.

Canada is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. The GOC has also ratified the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, the Inter-American Convention against Terrorism, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. On October 2, 2007, the GOC ratified the UN Convention against Corruption.

Canada is a member of the Financial Action Task Force (FATF) and underwent a mutual evaluation in early 2007. The results are expected to be released publicly via the FATF's website in 2008. Canada is a member of the Asia/Pacific Group on Money Laundering (APG), and also supports the Caribbean Financial Action Task Force (CFATF). Canada also belongs to the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. FINTRAC became a member of the Egmont Group in 2002. In June 2006, Toronto was selected as the permanent location of the Secretariat of the Egmont Group. The GOC will contribute approximately \$5 million over a five-year period to help establish the Secretariat.

Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2007, the GOC made strides in enhancing its anti-money laundering and counter-terrorist financing regime, and reducing its vulnerability to money laundering and terrorist financing. The GOC should continue to implement these efforts, particularly a system for administrative monetary penalties in 2008. The GOC should also ensure that its privacy laws do not excessively prohibit provision of information to domestic and foreign law enforcement that might lead to prosecutions and convictions. Such prohibitions also should not prohibit the exchange of information between FINTRAC and its counterpart FIUs, or information sharing on the cross-border movement of currency.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering and counter-terrorist financing regime. However, the islands remain vulnerable to money laundering due to their significant offshore sector. Most money laundering that occurs in the Cayman Islands is primarily related to fraud (particularly securities fraud), drug trafficking, and tax evasion.

The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance, investment funds, various types of trusts, and company formation and management. There are approximately 450 banks and trust companies, 8,600 funds, 740 captive insurance companies, and 62,572 exempt companies licensed or registered in the Cayman Islands. Shell banks are prohibited, as are anonymous accounts. Bearer shares can only be issued by exempt companies and must be immobilized. Gambling is illegal; and the Cayman Islands does not permit the registration of offshore gaming entities.

The Misuse of Drugs Law and the Proceeds of Criminal Conduct Law (PCCL) criminalize money laundering related to narcotics trafficking and all other serious crimes. A revision and consolidation of these laws has been proposed for enactment before the end of 2007. The PCCL provides for the offense of money laundering where a person or business has engaged in criminal conduct or has benefited from criminal conduct; tax offenses are not included. The PCCL was amended in May 2007 to incorporate terrorist financing offenses into the definition of money laundering.

The Cayman Islands Monetary Authority (CIMA) is responsible for the licensing, regulation and supervision of the Cayman Islands' financial industry, as well as monitoring the industry for compliance with its anti-money laundering and counter-terrorist financing (AML/CTF) obligations. The financial industry includes banks, trust companies, investment funds, fund administrators, insurance companies, insurance managers, money service businesses, and corporate service providers. These institutions, as well as most designated nonfinancial businesses and professions, are subject to the AML/CTF regulations set forth in the Guidance Notes on the Prevention and Detection of Money Laundering in the Cayman Islands (Guidance Notes). The Guidance Notes are issued by the CIMA and were last amended in May 2007. With the enactment of the Money Laundering (Amendment) (No 2) Regulation 2007 on August 7, 2007, dealers in precious metals and precious stones are now included in the definition of relevant financial businesses, but have been given a transitional grace period until January 1, 2008, for compliance. The real estate industry is also subject to AML/CTF regulations, but the CIMA does not have responsibility for supervising this sector.

The CIMA conducts on-site and off-site examinations of licensees. These examinations include monitoring for compliance with the PCCL and the CIMA's Guidance Notes. The Guidance Notes require employee training, record keeping, and "know your customer" (KYC) identification requirements for financial institutions and certain financial services providers. The regulations require due diligence measures for individuals who establish a new business relationship, engage in one-time transactions over 15,000 Cayman Islands dollars (approximately \$18,000), or who may be engaging in money laundering. The application of the AML/CTF measures to the financial sector and designated nonfinancial businesses is not based on risk assessment, although the CIMA does employ a risk-based approach to its on-site inspections.

The PCCL requires mandatory reporting of suspicious transactions, and makes failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. A suspicious activity report (SAR) must be reported once it is known or suspected that a transaction may be related to money laundering or terrorist financing. There is no threshold amount for the reporting of suspicious activity. It is currently not an offense to tip off the subject of a SAR; however, this should be corrected with the upcoming consolidation of the PCCL with the Misuse of Drugs Law that is currently underway.

Established under PCCL (Amendment) Law 2003, the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA is responsible for, among other things, receiving, analyzing, and disseminating SARs, including those relating to the financing of terrorism. The FRA began operations in 2004 and has a staff of six: a director, a legal advisor, a senior accountant, a senior analyst, a junior analyst, and an administrative officer. The FRA is a separate civilian authority governed by the Anti-Money Laundering Steering Group (AMLSG), which is

chaired by the Attorney General and includes as its members the Financial Secretary, the Managing Director of the Cayman Islands Monetary Authority, the Commissioner of Police, the Solicitor General, and the Collector of Customs. Obligated entities currently report suspicious activities to the FRA via fax, although the FRA plans to establish an electronic reporting system. Under the PCCL, the FRA has the authority to require all obligated entities to provide additional information related to a SAR.

The majority of SARs received by the FRA are submitted by banks, with 10 percent of the total SARs received submitted by lawyers. From July 1, 2006 to June 30, 2007 (the fiscal year of the FRA), the FRA received 219 SARs. As of August, the FRA had responded to nine requests for information from foreign FIUs in 2007, and sent an additional seven disclosures to foreign law enforcement or FIUs.

The Financial Crime Unit (FCU) of the Royal Cayman Islands Police (RCIP) is responsible for investigating money laundering and terrorist financing. The FCU works in conjunction with the Joint Intelligence Unit (JIU), which gathers and disseminates intelligence to domestic and international law enforcement agencies. The Legal Department of the Portfolio of Legal Affairs is responsible for prosecuting financial crimes. As of August, the FRA had sent two cases to the FCU for further investigation in 2007. There have been five money laundering convictions in the Cayman Islands since 2003.

On August 10, 2007, the Cayman Islands enacted the Customs (Money Declarations and Disclosures) Regulations, 2007. These regulations establish a mandatory declaration system for the inbound cross-border movement of cash and a disclosure system for money that is outbound. All persons transporting money totaling 15,000 Cayman Islands dollars (approximately \$18,000) or more into the Cayman Islands are required to declare such amount in writing to a Customs officer at the time of entry. Persons carrying money out of Cayman Islands are required to make a declaration upon verbal or written inquiry by a Customs officer.

The Cayman Islands has a comprehensive system in place for the confiscation, freezing, and seizure of criminal assets. In addition to criminal forfeiture, civil forfeiture is allowed in limited circumstances. Under the Misuse of Drugs Law and the PCCL, the courts can order the restraint of property upon application by a prosecutor. The FRA can also request a court order to freeze bank accounts if it suspects the account is linked to money laundering or terrorist financing. However, while the police may obtain production orders for the purposes of investigation and confidential information, there are no specific asset-tracing provisions. These will be provided for in the proposed consolidation of the PCCL and the Misuse of Drugs Law. Over \$120 million in assets has been frozen or confiscated since 2003.

The Cayman Islands is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the United Kingdom has yet to extend the application of the International Convention for the Suppression of the Financing of Terrorism to the Cayman Islands. The Cayman Islands criminalized terrorist financing through the passage of the Terrorism Bill 2003, which extends criminal liability to the use of money or property for the purposes of terrorism. It also contains a specific provision on money laundering related to terrorist financing. While lists promulgated by the UN Sanctions Committee and other competent authorities are legally recognized, there is no legislative basis for independent domestic listing and delisting. The confiscation, freezing, and seizure of assets related to terrorist financing are permitted by law. Nonprofit organizations must be licensed and registered, although there is no competent authority responsible for their supervision. There have been no terrorist financing investigations or prosecutions to date in the Cayman Islands.

In 1986, the United States and the United Kingdom signed a Treaty concerning the Cayman Islands relating to Mutual Legal Assistance in Criminal Matters. By a 1994 exchange of notes, Article 16 of that treaty has been deemed to authorize asset sharing between the United States and the Cayman Islands. The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF). In

June 2007, CFATF conducted its third mutual evaluation of the Cayman Islands. The evaluation team found the Cayman Islands to be compliant or largely compliant with 38 of the 49 Financial Action Task Force recommendations. The FRA is a member of the Egmont Group. The FRA currently has nine MOUs with FIUs in Australia, Canada, Chile, Guatemala, Indonesia, Mauritius, Nigeria, Thailand, and the United States.

The Government of the Cayman Islands should continue its efforts to implement its anti-money laundering and counter-terrorist financing regime. It should enact the proposed provisions to consolidate the Misuse of Drugs Law and the Proceeds of Criminal Conduct Law to criminalize tipping off the subjects of suspicious activity reports and to allow for asset tracing provisions. The Caymans Islands should also ensure that new provisions related to AML/CTF requirements for dealers in precious metals and stones and the disclosure/declaration system for the cross-border movement of currency are fully implemented.

Chile

Chile's has a large and well-developed banking and financial sector. The government is actively seeking to turn Chile into a global financial center and has signed 55 Free Trade Agreements with countries around the world. With the increase in legitimate trade and currency flows and the growing economy may come an increase in illicit activity and money laundering. Stringent bank secrecy laws emphasizing privacy rights have been broadly interpreted and hamper Chilean efforts to identify and investigate money laundering and terrorist financing. Chile's incomplete and still-developing regulatory oversight is an additional vulnerability.

In 2007, the Government of Chile (GOC) prosecuted its first four money laundering cases under the new penal system. In the first case, the defendant was found guilty of drug trafficking, but not money laundering. However, the sentence he received included the seizure of all his assets, not solely those tied to narcotics trafficking; thus, while not convicted of money laundering, he received the penalty associated with a money laundering conviction. The second and third cases were resulted in conviction on charges of money laundering as a result of plea bargaining, marking the first two recorded money laundering convictions under the new penal system. The fourth case, however, resulted in a conviction of money laundering by the trial judges. The accused in this case laundered money from the proceeds of drug trafficking in Europe and was sentenced to six years in prison, with all of his assets confiscated.

Chile criminalized money laundering under Law 19.366 of 1995, Law 19.913 of 2003, and Law 20.119 of 2006. Under Law 19.913, predicate offenses for money laundering include narcotics trafficking, terrorism in any form and the financing of terrorist acts or groups, illegal arms trafficking, kidnapping, fraud, corruption, child prostitution and pornography, and some instances of adult prostitution. Chile has yet to widen the scope of money laundering to apply it to other types of crimes such as trafficking in persons, intellectual property rights violations, and extortion. Detection methods, particularly when not tied to drug trafficking, are still weak. Thus, while most money laundering thus far discovered is tied to drug dealing, it is difficult to determine whether the majority of money laundering in Chile truly is tied to this crime.

Law 19.913 created Chile's financial intelligence unit, the Unidad de Análisis Financiero (UAF), as an autonomous agency affiliated with the Ministry of Finance. The UAF currently has a staff of 21, and has received approval in the budget for 2008 to expand to 31 employees. Law 19.913 requires mandatory reporting of suspicious transactions to the UAF by banks and financial institutions, financial leasing companies, general and investment funds-managing companies, pension fund administration companies, the Foreign Investment Committee, money exchange firms and other entities authorized to receive foreign currencies, firms that carry out factoring operations, credit card issuers and operators, securities companies, money transfer and transportation companies, stock

exchanges, stock exchange brokers, securities agents, insurance companies, mutual funds managing companies, forwards and options markets operators, tax-free zones' legal representatives, casinos, gambling houses and horse tracks, customs general agents, auction houses, realtors and companies engaged in the land development business, notaries and registrars. Law 20.119 now also subjects pension funds and sports clubs to reporting requirements. Dealers in jewels and precious metals, and intermediaries (such as lawyers and accountants) are not subject to reporting requirements.

In addition to filing suspicious transaction reports (STRs), Law 19.913 also requires that obligated entities maintain registries of cash transactions that exceed 450 unidades de fomento (UF) (approximately \$17,000). All cash transaction reports (CTRs) contained in the internal registries must be sent to the UAF at least once a year, or more frequently at the request of the UAF. The UAF requires banks to submit CTRs every month, and money exchange houses and most other obliged institutions every three months. Some specific institutions without a high amount of cash transactions (e.g. notaries) may submit CTRs every 6 months. In all cases, institutions must report CTRs dating from May 2004, when the obligation to record cash transactions over 450 UF went into effect. As of September, the UAF had received 1,839 CTRs and 301 STRs in 2007.

The Chilean tax service (Servicio de Impuestos Internos) issued a regulation, Resolution 120, requiring all banks, exchange houses and money remitters to report all transactions exceeding \$10,000 sent to or received from foreign countries. Twenty-four banks joined together to appeal this regulation, claiming compliance would violate bank secrecy and expose them to lawsuits. The court of appeals ruled in favor of the banks, which are no longer subject to Resolution 120. The physical transportation of cash exceeding \$10,000 into or out of Chile must be reported to Customs, which then files a report with the UAF. These reports are sent to the UAF daily. However, Customs and other law enforcement agencies are not legally empowered to seize or otherwise stop the movement of funds, and the GOC does not impose a significant penalty for failing to declare the transportation of currency in excess of the threshold amount.

Law 20.119 authorizes the UAF to impose sanctions on obligated entities for noncompliance with requirements to establish an anti-money laundering and counter-terrorist financing (AML/CTF) system or reporting suspicious/cash transactions. In 2007, the UAF identified several cases of failure to report suspicious activity or to establish an AML/CTF system. It sanctioned some nonbank financial institutions for the first time this year by either fining the institution, or by sending it a letter stating the institution was sanctioned. If the organization is not found to be compliant within a year, it can be subject to three times the maximum fine for being sanctioned twice in a year. The UAF may also access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. The UAF does not have regulatory responsibilities, but can issue general instructions on reporting obligations, such as requiring reporting entities to report any transactions by persons suspected of terrorist financing.

The Superintendence of Banks and Financial Institutions (SBIF) supervises banks in Chile, and stock brokerages, securities firms, and insurance companies are under the supervision and regulation of the Superintendence of Capital Markets. Chile's anti-money laundering laws oblige banks to abide by "know-your-customer" standards and other money laundering controls for checking accounts. However, the same compliance standards do not apply to savings accounts. Only a limited number of banks rigorously apply money laundering controls to noncurrent accounts. Banks and financial institutions must keep records with updated background information on their clients throughout the period of their commercial relationship, and maintain records for a minimum of five years on any case reported to the UAF. The UAF has expressed concern about the quality of STRs, but is the organization responsible for working with reporting entities to improve quality. Bank compliance officers complain that, while the UAF has criticized the quality of their reports, it has provided no training to teach them how to improve. The UAF and the Banking Association have asked representatives from Colombia's FIU to provide training to the banks in 2008. None of the money

laundering cases that have gone to trial in Chile to date were referred by the UAF, nor did they contain evidence provided by banks, though money passed through banks in all of the cases.

Insufficient supervision and the lack of a definition of “suspicious activity” for nonbank and nonfinancial institutions continue to be identified as deficiencies in the GOC’s AML/CTF regime. Each entity independently decides what constitutes irregularities in financial transactions. Nonbank financial institutions, such as money exchange houses and cash couriers, do not fall under the supervision of any regulatory body for compliance with AML/CTF standards. In Santiago alone there are more than 60 exchange houses (approximately 114 nationwide), many of which do not record or share with other exchange houses any information about their customers. The GOC is aware of the need for regulation of these entities. As of May 2007, nonbank financial institutions must obtain contact information and a declaration of origin statement from individuals carrying out transactions of more than \$5,000. These institutions must also report transactions of up to \$4,999 to the UAF if they are considered to be suspicious. Nevertheless, the lack of supervision, training in the definition of “suspicious activity,” and a harmonized system to keep record of daily transactions diminishes useful reporting to the UAF and undermines the effectiveness of the system. This sector appears particularly vulnerable to abuse by money launderers.

Chile’s gaming industry falls under the supervision of the Superintendence of Casinos (SCJ), which is in charge of drafting regulations about casino facilities, and the administration, operation and proper development of the industry. Online gambling is prohibited except for the Internet purchase of lottery tickets from one of Chile’s two lotteries. Eight casinos are currently operating throughout the country. The SCJ has oversight powers and regulatory authority over the industry but no law enforcement authority. Under Law 19.995, the SCJ granted authorization for 15 casinos to operate in Chile after participating in an international and domestic bidding process to assign permits during 2005 and 2006. One new casino opened in 2007, and nine are expected to open in 2008. By 2009, a total of 22 casinos will be fully operational and under the oversight authority of the SCJ. The SCJ screened applications for the new casino licenses with the support of domestic and international police and financial institutions. However, Chilean law limits the SCJ to 270 days for the entire background check and determination of whether to issue a license.

Law 19.913 requires casinos to keep a record of all cash transactions over UF 450 (the equivalent of approximately \$17,000), and to designate a compliance officer. However, in July 2007, the UAF instructed casinos to identify, know, and maintain records on all customers—Chileans and foreigners—who carry out any transaction over \$3,000. The SCJ also requires the casinos to prepare and submit for approval manuals detailing their AML/CTF plan. The SCJ is working to establish additional regulations, internal control standards, and standardized forms to improve their ability to monitor the growing number of casinos. Chile’s Finance Ministry, in cooperation with the SCJ, presented to Congress a draft law addressing some of the weaknesses of Chile’s gaming law. The draft law, if it passes, will provide increased regulatory authority to the SCJ and prohibit individuals without licenses from operating electronic gambling games.

When the UAF determines that an account or a case requires further investigation, it passes the information to the Public Ministry (the public prosecutor’s office). The Public Ministry is responsible for receiving and investigating all cases from the UAF and has up to two years to complete an investigation and begin prosecution. In 2007, the UAF referred seven cases to the Public Ministry.

The Public Ministry’s unit for money laundering and economic crimes has been proactive in investigating crimes, and pursuing training opportunities to further educate its prosecutors and other players in the criminal justice process. The money laundering unit is also developing a manual for prosecutors trying drug cases. The manual provides practical steps to investigate assets so as to identify possible money laundering as well as drug trafficking. They have also established a computer

link with the tax service, SBIF, and other relevant agencies to access information that is not protected by bank and tax secrecy laws.

The Chilean investigative police (PICH) and the uniformed national police (Carabineros) work in conjunction with the Public Ministry on money laundering investigations. They also cooperate with U.S. and regional law enforcement in money laundering investigations. In 2004, Customs agents at Santiago's airport alerted the newly formed UAF of cash couriers bringing large amounts of euros to Chile from Colombia. After analysis, the UAF referred the case to the CDE (the precursor to the Public Ministry), which formally opened an investigation. The PICH's anti-money laundering unit and DEA uncovered an international money laundering scheme in which employees of some cash exchange houses carried euros and U.S. dollars from Colombia to Chile. The money was then carried by Chilean employees on commercial flights to the United States where it was deposited in banks and returned to Colombia in pesos. Through Chilean/DEA cooperation, arrests were made in Chile and the U.S. simultaneously and the money laundering ring was broken.

The police are competent and well-trained, but many are new to investigating financial crimes. Many complain of insufficient access to information. Chilean law prohibits the UAF from giving information directly to law enforcement, and allows the sharing of information only with the Public Ministry and foreign FIUs. Currently police must request financial information from the Public Ministry, which in turn requests it from the UAF. The UAF responds with all available information; however, much financial and tax information is protected through Chile's strict secrecy laws.

Bank secrecy is the most often identified obstacle to money laundering investigations identified by the police and prosecutors. Article 154 of the General Banking Law states that deposits and obligations of any kind shall be subject to banking secrecy, and information about such transactions may only be provided to the depositor or creditor (or an authorized legal representative). Law 707 also states that banks may not share information about the movement and balances in a current account with a third party. To avoid possible lawsuits, banks do not share information with prosecutors unless the prosecutors produce a judicial order. Thus, bank compliance officers are restricted to simply reporting suspicious activity and then waiting for the appropriate court authorization to release any private information. Many banks respond quickly to requests for information from the UAF, but are slow to reply to judicial court orders to provide prosecutors with additional information. When they do reply, they often provide incomplete information. Police and prosecutors complain they lose valuable time waiting at least a month (but usually more) for banks to provide incomplete information. Judges can require the detention of the bank's general manager until all information is disclosed, but this tool is rarely used. In the instances when the judge has issued the order for the general manager's detention, bank information was provided immediately.

Under Law 20.119, the Public Ministry can, with the authorization of a judge, lift bank secrecy provisions to gain account information if the account is directly related to an ongoing case. Unless a suspicious transaction report has been filed on an account, prosecutors and the UAF must get permission from a judge to examine an account. The process is often subject to the determination of judges who have received little training in financial crimes. The judges must decide if the prosecutors have presented sufficient evidence to warrant lifting bank secrecy. However, this process often prohibits prosecutors and the UAF from accessing the information they would need to convince a judge of suspicious activity. The UAF has made approximately 10 requests per year, petitioning a judge only when confident the request would be granted. All requests have been granted within 24 hours, but the system does not yet encourage aggressive examination of suspicious activity on the part of the UAF, and time is lost in the preparation of the case for the judge.

A draft law currently under discussion in a committee of Chile's House of Representatives would facilitate easier access to bank and tax records for the UAF and prosecutors in certain instances. If passed, this law would bring Chile more into greater compliance with the Financial Action Task Force

(FATF) Recommendations, and UN resolutions on terrorist financing. The draft law has been sitting in the Congressional commission since it was introduced in May 2007. Without urgent status granted to it by the President, it appears unlikely to work its way through the legislative process quickly. The Organization for Economic Cooperation and Development (OECD), to which Chile hopes to accede, criticized Chile's bank secrecy laws in October 2007. Chile's Foreign Minister used the opportunity to encourage passage of the draft law.

Law 19.913 contains provisions that allow prosecutors to request that assets be frozen only when tied to drug trafficking. No provisions have been made for freezing assets under other circumstances, including assets of individuals or companies designated by UN Security Council Resolution 1267. The Ministry of National Property currently oversees forfeited assets, and proceeds from the sale of forfeited assets are passed directly to CONACE, the National Drug Control Commission, to fund drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Chilean law does not permit the seizure of substitute assets or civil forfeiture. The same draft law that would facilitate lifting bank secrecy for the UAF and Public Ministry would allow for the freezing of assets in cases of suspected terrorist financing and would enable Chile to share seized assets with other governments. The draft law would also ensure assets seized in money laundering convictions would go, at least in part, to law enforcement rather than only to drug rehabilitation programs. A total of \$2 million in assets were seized in money laundering investigations in 2007.

Two free trade zones exist in Chile, in Punta Arenas and Iquique. The Iquique free trade zone, the larger of the two, also has an extension in Arica, near Chile's border with Peru. The physical borders of the free trade zone are porous and largely uncontrolled. All companies in the free trade zone are reporting entities and must report any suspicious activity to the UAF. Due to weak detection methods, determining the extent of money laundering in the free trade zones is virtually impossible. Iquique appears to be the primary conduit for counterfeit goods into Chile, and one of the main conduits of counterfeit goods moving to the Tri-Border Area between Brazil, Paraguay, and Argentina. Chilean resources to combat this issue are extremely limited. Police investigative efforts suggest possible criminal links between Iquique and the Tri-Border Area involving both terrorist financing of Hizballah and Hamas and money laundering.

Law 18.314 and Law 19.906 criminalize terrorist financing in Chile. Law 19.906 modifies Law 18.314 to more efficiently sanction terrorist financing in conformity with the UN International Convention for the Suppression of the Financing of Terrorism. Under Law 19.906, financing a terrorist act and the provision (directly or indirectly) of funds to a terrorist organization are punishable by five to ten years in prison. The Superintendence of Banks circulates the UNSCR 1267 Sanctions Committee's consolidated list to banks and financial institutions. The UAF also posts the 1267 list on its website and has instructed all reporting entities to report any transactions by those on the list. The GOC has not identified any terrorist assets belonging to individuals or groups named on the list to date in Chile. Law enforcement lacks tools to investigate terrorist financing; undercover operations, for example, are not permitted for such investigations.

The GOC does not monitor transactions outside of Chile to prevent terrorist financing, nor does it regulate nongovernmental organizations (NGOs). Nonprofit organizations must register at the Justice Ministry, but this Ministry has no regulatory responsibility over them. In response to the evaluation of Chile by the Financial Action Task Force of South America (GAFISUD), which was released in December 2006, the Finance Ministry initiated discussions with the Superintendence of Banks and the Superintendence of Capital Markets to identify the best way to monitor NGOs; these discussions have not yet reached conclusions.

Chile is party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN

Convention against Corruption, and the Inter-American Convention on Terrorism. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. The UAF is a member of the Egmont Group of financial intelligence units and serves as one of the representatives for the Americas on the Egmont Committee. The UAF has signed memoranda of understanding (MOUs) for the exchange of financial information with the United States FIU and FIUs of 32 other jurisdictions.

The GOC is proactive in pursuing partnerships with other countries. It signed an agreement with Colombia in 2007 to cooperate on terrorism and economic crimes. There is no regular, formal exchange of records with the United States, but case-specific cooperation and exchange of records is very strong. Negotiations with Chile on the FBI's South American Fingerprint Exploitation (SAFE) project, whereby Chile and U.S. would share fingerprint records of criminals, are ongoing. As part of Chile's strategy to access the OECD, Chile participates, as an observer or invitee, in 18 OECD Committees and Working Groups, including the Working Group on Bribery and Transnational Crimes.

The first money laundering conviction by judges under the new judicial system demonstrates a significant step in the Government of Chile's anti-money laundering regime. However, it remains to be seen if the system will be successful in convicting money launderers without ties to drug trafficking. Issues of limited access to information for the Public Ministry, the PICH, and the Carabineros and inter-agency conflict should be resolved. Reporting entities should be adequately supervised, receive sufficient training in determining suspicious activity, and monitored for compliance with reporting requirements. The GOC should ensure the passage of the draft law currently sitting in the lower house of Congress to allow for the lifting of bank secrecy and the freezing of assets. Passage of this law would bring Chile closer to compliance with its UNSCR 1267 obligations and FATF Recommendations. The GOC should also increase government oversight of nonfinancial institutions, allow for greater access to information for the UAF and other key agencies, and enhance inter-agency cooperation to improve Chile's ability to combat money laundering and terrorist financing.

China, People's Republic of

Over the past five years, the Government of the People's Republic of China has made significant progress in developing anti-money laundering and counter-terrorist financing measures including through legislative reform, strengthening enforcement mechanisms, and international cooperation efforts. However, money laundering remains a serious concern as China restructures its economy and develops its financial system. Narcotics trafficking, smuggling, trafficking in persons, counterfeiting of trade goods, fraud, tax evasion, and other financial crimes are major sources of laundered funds. Most money laundering cases currently under investigation involve funds obtained from corruption and bribery. Chinese officials have noted that most acts of corruption in China are closely related to economic activities and accompanied by illegal money transfers. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment and, as such, receive tax benefits. Underground banking and trade-based money laundering are an increasing concern. According to the International Monetary Fund, money laundering in China may total as much as U.S. \$24 billion per year and officials with the People's Bank of China reported a total of 1,239 cases involving illicit money flows involving 362.6 billion Chinese yuan renminbi (RMB) (approximately U.S. \$45.3 billion) in 2006.

The People's Bank of China (PBC), China's central bank, maintains primary authority for anti-money laundering and counter terrorist finance coordination. The PBC also shares some anti-money laundering responsibilities with other financial regulatory agencies, including: the China Banking Regulatory Commission (CBRC), which supervises and regulates banks, asset management

companies, trust and investment companies, and other deposit-taking institutions; the China Insurance Regulatory Commission (CIRC), which supervises the insurance sector; and the China Securities Regulatory Commission (CSRC), which supervises the securities sector. The Ministry of Public Security's Anti-Money Laundering Division and Anti-Terrorism Bureau lead anti-money laundering and counter-terrorist finance-related law enforcement efforts.

Within the PBC's Financial Intelligence Unit (FIU), the Anti-Money Laundering Bureau (AMLB) handles the coordination of all anti-money laundering programs and carries out administrative and policy oversight, while the China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) collects, analyzes, and disseminates suspicious transaction reports and currency transaction reports. According to CAMLMAC, which was established in 2004, 683 reports on suspicious transactions, involving RMB 137.8 billion (approximately U.S. \$18.9 billion), were identified for further investigation by the end of 2005. From July 1, 2005 to June 30, 2006, CAMLMAC received 619,962 RMB suspicious transaction reports and 2,245,267 foreign currency suspicious transactions. The 2007 FATF mutual evaluation of China noted that consideration should be given to the problem of how to effectively manage and exploit such a large volume of STRs coming directly to CAMLMAC, which has a staff of only sixty people.

Since its inception, the FIU has transferred 57 files (involving about 80,000 separate suspicious transactions) to the Ministry of Public Security (MPS) for investigation. Nine referrals have resulted in cases being filed for investigation; and one has been referred for prosecution. Since October 2005, approximately ten suspicious transaction dossiers have been transferred to other agencies, including five to the Ministry of State Security (MSS). Four of these cases are still being investigated by the MSS. The other referral was closed after investigation.

The MPS is China's main law enforcement body, responsible for following up on STRs and for guiding and coordinating public security authorities across China in investigations involving money laundering and the seizure, freezing and confiscation of proceeds of crime. Most of these responsibilities are concentrated in the AML Division of the MPS Economic Crime Investigation Department (ECID). The Anti-Terrorism Bureau of the MPS is responsible for investigating general crimes relating to terrorist financing. Crimes against state security (including terrorism and related crimes) are the responsibility of the Ministry of State Security (MSS). The Supreme People's Procuratorate (SPP) supervises and directs the approval of arrests, prosecution, and supervision of cases involving money laundering crimes. The Supreme People's Court (SPC) supervises and directs the trial of money laundering crimes. Both can issue judicial interpretations. Law enforcement agencies are authorized to use a wide range of powers, including special investigative techniques, when conducting investigations of money laundering, terrorist financing and predicate offences. These powers include seizing articles relevant to the crime, including all (customer) records held by financial institutions. Reportedly, law enforcement and prosecutorial authorities currently focus on pursuing predicate offences, to the exclusion of AML/CTF.

China has criminalized money laundering under three separate articles of the Penal Code. Article 349 of the Penal Code was introduced in December 1990 to criminalize the laundering of proceeds generated from drug-related offenses. In June 2006, Article 191 of the Penal Code was amended to expand the criminalization of money laundering to seven predicate offenses, which now include fraud, bribery, and embezzlement, in addition to narcotics trafficking, organized crime, smuggling, and terrorism. Article 312 was also amended in June 2006 to make it an offense to launder the proceeds of any crime through a variety of means, and it criminalizes complicity in concealing the proceeds of criminal activity.

A new Anti-Money Laundering Law, which covers AML/CTF preventative measures for the entire financial system, took effect January 1, 2007. The law broadened the scope of existing anti-money laundering regulations by mandating that financial institutions maintain thorough records on accounts

and transactions, and report large and suspicious transactions. These actions firmly established the PBC's authority over national anti-money laundering efforts.

The PBC executed a revised regulatory framework in early 2007 to support the new Anti-Money Laundering Law. "Rules for Anti-Money Laundering by Financial Institutions" (AML Rules) took effect January 1, 2007, and "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions" (LVT/STR Rules) took effect March 1, 2007. Under the revised rules, all financial institutions—including securities, insurance, trust companies and futures dealers are considered accountable for managing their own anti-money laundering mechanisms and must report large and suspicious transactions. The LVT/STR Rules were amended on June 21, 2007 to require financial institutions to report suspicious transactions related to terrorist financing.

Under the AML and LVT/STR Rules, any cash deposit or withdrawal of over RMB 200,000 or foreign-currency withdrawal of over U.S. \$10,000 in one business day must be reported within five days electronically or within 10 days in writing to the PBC Financial Intelligence Unit. Money transfers between companies exceeding RMB 2 million (approximately U.S. \$274,000) in one day or between an individual and a company greater than RMB 500,000 (approximately U.S. \$68,500) must also be reported. The new rules also require that all financial institutions submit monthly reports outlining suspicious activities and retain transaction records for five years. Financial institutions that fail to meet reporting requirements in a timely manner are subject to a range of administrative penalties and sanctions including having their licenses or business operations suspended.

The Administrative Rules for Financial Institutions on Customer Identification and Record Keeping of Customer Identity and Transaction Information (CDD Rules) became effective on August 1, 2007. These rules require all financial institutions to identify and verify their customers, including the beneficial owner. Specific requirements relating to the identification of legal persons (e.g. requirements to verify their legal status by obtaining proof of incorporation) have been extended to all financial institutions. The CDD Rules also introduce specific requirements for financial institutions in relation to foreign Politically Exposed Persons (PEPs), including having to obtain approval from senior management before opening an account and determining the source of funds.

China has implemented a cross-border disclosure/declaration system operated by the General Customs Administration (GCA). All cross-border transportations of cash exceeding RMB 20,000 for local currency (approximately U.S. \$2,740) or for foreign currency must be declared. Bearer negotiable instruments do not need to be declared, but cross-border transportation of RMB through the mail system or in vehicles is not permitted. China has also implemented a disclosure system based on a risk-based targeting system. The GCA is authorized to conduct checks of persons entering or leaving the country, seize undeclared cash, and question, detain and sanction anyone who violates any requirement. Those who carry out physical cross border transportation related to money laundering or terrorist financing are also subject to criminal sentences. New provisions allowing the use of RMB in Hong Kong have also created loopholes for money laundering activity. From January 2005 to October 2006, there were 4,926 cases involving travelers who did not disclose cash being carried, but this data is not effectively being utilized for money laundering or terrorist financing investigations. .

China's cash-based economy, combined with robust cross-border trade, contributes to a high volume of difficult-to-track large cash transactions. While China is proficient in tracing formal financial transactions, the large size of the informal economy—estimated by the Chinese Government at approximately ten percent of the formal economy, but quite possibly much larger—means that tracing informal financial transactions presents a major obstacle to law enforcement. Anti-money laundering efforts are further hampered by the prevalence of counterfeit identity documents and underground banks, which in some regions reportedly account for over one-third of lending activities. Only banks are authorized to provide money or value transfer services in China. Banks are not allowed to have agents that could offer such services. According to Article 174 of the Penal Code, it is a criminal offense to operate an illegal financial institution or provide financial services illegally in China.

Authorities have expressed concern that criminal or terrorist groups could exploit underground banking mechanisms to bypass law enforcement. According to the FATF, China has had some success at combating illegal underground banking. Authorities destroyed 47 underground banks in 2005; in 2006, Chinese police uncovered seven underground banks and seized laundered assets totaling more than 14 billion RMB (approximately U.S. \$1.92 billion).

The extent of underground banking's link to the large expatriate Chinese community is not known. Traditionally, "flying money" or fei-chien networks, are operated by money changers, gold shops, and trading companies. The international Chinese underground banking system is dependent on close associations and family ties that are resistant to most law enforcement countermeasures. Value transfer via trade goods, including barter exchange, is a common component in Chinese underground finance. Many Chinese underground trading networks in Africa, Asia, the Middle East, and the Americas are involved in the trade of Chinese-manufactured counterfeit goods, in violation of intellectual property rights. There are reports that the proceeds of narcotics produced in Latin America are laundered via trade by purchasing Chinese manufactured goods (both licit and counterfeit) in an Asian version of the Black Market Peso Exchange.

To remedy information deficiencies, the PBC launched a national credit-information system in January 2006. Although still very limited, this system allows banks to have access to information on individuals as well as on corporate entities. The new Anti-Money Laundering Law also explicitly prohibits financial institutions from opening or maintaining anonymous accounts or accounts in fictitious names, and PBC rules obligate financial institutions to perform customer due diligence, regardless of the type of customer (business or individual), type of transaction, or level of risk.

To address online fraud, the PBC has tightened regulations governing electronic payments. In 2005, the PBC announced new rules prohibiting consumers from making online purchases of more than RMB 1,000 (approximately U.S. \$137) in any single transaction or more than RMB 5,000 (approximately U.S. \$688) in a single day. Enterprises are limited to electronic payments of no more than RMB 50,000 (approximately U.S. \$6,900) in a single day. In March 2007, Chinese regulators announced additional online restrictions regarding the use "virtual money;"—online credits sold by websites to customers to pay for games and other web-based services—amidst rumors that such credits were being used to launder money.

China is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. In 2006, China became a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Corruption.

China has signed mutual legal assistance treaties with over 24 countries and has entered into some 70 MOUs and cooperation agreements with over 40 countries. The United States and China signed a mutual legal assistance agreement (MLAA) in June 2000, the first major bilateral law enforcement agreement between the countries. The MLAA entered into force in March 2001 and provides a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The United States and China cooperate and discuss money laundering and enforcement issues under the auspices of the U.S./China Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. In addition, the United States and China have established a Working Group on Counterterrorism that meets on a regular basis. China has established similar working groups with other countries as well.

China has signed extradition agreements with 30 countries to make it more difficult for economic criminals to seek shelter abroad. According to China's Ministry of Public Security, approximately 800 Chinese economic crime suspects have reportedly fled abroad with more than 70 billion RMB (approximately U.S. \$9.1 billion) involved.

In late 2004, China joined the Eurasian Group (EAG), a FATF-style regional body that includes Russia, Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. In January 2005, China

became an observer to the FATF and gained full membership in June 2007. FATF published its Mutual Evaluation Report on China in June 2007. China's FIU has applied for membership to the Egmont Group.

Subsequent to the September 11, 2001, terrorist attacks in the United States, Chinese authorities began to actively participate in U.S. and international efforts to identify, track, and intercept terrorist finances, specifically through implementation of United Nations Security Council counter-terrorist financing resolutions. According to the FATF, China has not implemented UNSCR 1267 and UNSCR 1373 in a manner that meets the specific requirements of FATF Special Recommendation III. China's primary domestic concerns with terrorist financing focus on the western Xinjiang Uighur Autonomous Region. Terrorist financing is a criminal offense in China. However, the terrorist financing laws lack clarity in a number of critical areas.

The Chinese Government significantly strengthened its anti-money laundering regime through legislative and regulatory reforms, law enforcement mechanisms, and membership in international organizations, in particular the FATF. The Chinese Government should continue to build upon actions taken in recent years to develop a viable anti-money laundering/counter-terrorist financing regime consistent with international standards. Important steps include expanding the list of predicate crimes to include terrorism, including terrorist financing, as a predicate offense. China should continue to develop a regulatory and law enforcement environment designed to prevent and deter money laundering, and it should raise awareness within the judiciary of money laundering as a criminal offense. China should ensure that law enforcement and prosecutorial authorities specifically pursue money laundering and terrorist financing offenses, and not simply treat them as a subsequent byproduct of investigations into predicate offenses. China's Anti-Money Laundering Law and related regulations should also apply to a broader range of nonfinancial businesses and professions. The application of sanctions for noncompliance with requirements that financial institutions perform customer identification, due diligence, and record keeping should be assessed to ensure that they have a genuinely dissuasive effect. In addition to strengthening its counter-terrorism finance regime, Chinese law should specifically define the term "terrorist activities" to be consistent with international standards. The Penal Code should also specify the definition of "funds" and criminalize the act of collecting funds for terrorist purposes. In addition, China should strengthen its mechanisms for freezing terrorist assets. Chinese law enforcement authorities should examine domestic ties to the international network of Chinese expatriate brokers and traders that are often linked to underground finance, trade fraud, and trade-based money laundering.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Comprehensive anti-money laundering regulations have allowed the government to refine and improve its ability to combat financial crimes and money laundering. Nevertheless, the laundering of money from Colombia's lucrative cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. Although progress has been made in recent years, a complex legal system and limited resources for anti-money laundering programs constrain improvements. Laundering illicit funds is related to a number of criminal activities (narcotics trafficking, commercial smuggling for tax and import duty evasion, kidnapping for profit, and arms trafficking and terrorism connected to violent paramilitary groups and guerrilla organizations), and is carried out, to a large extent, by U.S. Government-designated terrorist organizations. The GOC and U.S. law enforcement agencies closely monitor transactions that could disguise terrorist finance activities. The U.S. and Colombia exchange information and cooperation based on Colombia's 1994 ratification of the United Nations Convention against Illicit Trafficking in Narcotics and Psychotropic Substances. This convention extends into most money laundering activities resulting from Colombia's drug trade.

Colombia's economy is robust and diverse and is fueled by significant export sectors that ship goods such as coal, petroleum products, textiles and apparel, flowers, and coffee to the U.S. and beyond. While Colombia is not a regional financial center, the banking sector is mature and well regulated. An increase in financial crimes not related to money laundering or terrorist financing, such as bank fraud, has not been widely seen in Colombia. However, criminal elements have used the banking sector to launder money, under the guise of licit transactions. Money laundering has occurred via trade and the nonbank financial system, especially related to transactions that support the informal or underground economy. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds.

Casinos in Colombia lack adequate regulation and transparency. Free trade zones in some areas of the country present opportunities for smugglers to take advantage of lax customs regulations, or the corruption of low-level officials to move products into the informal economy. Although corruption of government officials remains a problem, its scope has decreased in recent years. The GOC continues to implement steps to ensure the integrity of its most sensitive institutions and senior government officials.

Money launderers in Colombia employ a wide variety of techniques, and frequently use such methods as the Black Market Peso Exchange and contraband trade to launder the proceeds of illicit activities. Colombia's financial intelligence unit (FIU), the Financial Information and Analysis Unit (Unidad de Información y Análisis Financiero or UIAF) has identified more than ten techniques alone for laundering money via contraband trade. Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency and EU euros. Local currency exchangers convert narcotics currency to Colombian pesos and then ship the U.S. dollars and euros to Central America and elsewhere for deposit as legitimate exchange house funds that are then reconverted to pesos and repatriated by wire to Colombia. Other methods include the use of debit and stored value cards to draw on financial institutions outside of Colombia and the transfer of funds out of and then back into Colombia by wire through different exchange houses to create the appearance of a legal business or personal transaction. Colombian authorities have also noted increased body smuggling (carrying currency on a person) of U.S. and other foreign currencies and an increase in the number of shell companies operating in Colombia. Pre-paid debit and stored value cards, Internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia.

Colombia has broadly criminalized money laundering. Under legislation passed in 1995, 1997, and 2001, the GOC has established the "legalization and concealment" of criminal assets as a separate criminal offense, and criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, narcotics trafficking, arms trafficking, crimes against the financial system or public administration, and criminal conspiracy. Under a new law approved in 2006, penalties under the criminal code for money laundering and terrorist financing range from eight to 22 years with fines from 650 to 50,000 times the current legal minimum salary. Persons who acquire proceeds from drug trafficking are subject to a potential sentence of six to fifteen years, while illicit enrichment convictions carry a sentence of six to ten years. Failure to report money laundering offenses to authorities is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials, since under Colombian law there is a legal exemption to client confidentiality when a financial institution suspects money laundering activity. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments and private consultants to ensure system integrity. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Obligated

entities are supervised by the Superintendence of Finance. In 2007, the Superintendence of Finance issued a circular requiring entities under its authority to implement a new consolidated risk monitoring system that includes risk prevention and control measures based on international standards by January 1, 2008.

Established in 1999 within the Ministry of Finance and Public Credit, the UIAF is widely viewed as a hemispheric leader in efforts to combat money laundering and supplies considerable expertise in organizational design and operations to other FIUs in Central and South America. The UIAF has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities, which include banks, stock exchanges and brokers, mutual funds, investment funds, export and import intermediaries, credit unions, wire remitters, exchange houses, public agencies, notaries, casinos, lottery operators, car dealers, and foreign currency traders, are required to report suspicious transactions to the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish “know-your-customer” provisions. With the exception of exchange houses, obligated entities must report to the UIAF cash transactions over U.S. \$5,000. The UIAF requires exchange houses to provide data on all transactions above U.S. \$200. In 2007, 7,136 suspicious transaction reports (STRs) were filed through the month of September, with 58 percent of STRs deemed by UIAF to merit further investigation by their analysis unit. The Fiscalía (National Prosecutor’s Office) reported 48 convictions for money laundering in 2007.

In 2006, the UIAF inaugurated a new centralized data network connecting 15 governmental entities as well as the banker’s association (Asobancaria). The network allows these entities to exchange information online and share their databases in a secure manner, and facilitates greater cooperation among government agencies in preventing money laundering and other financial crimes. As of October 2007, the UIAF’s database contained over 525 million transaction and activity reports. Between 2000 and September 2007, the UIAF provided authorities with 610 financial intelligence reports pertaining to 32,774 individuals, 2,031 businesses, and approximately U.S. \$3.5 billion in transactions.

Given concerns about bulk cash smuggling, the GOC requires individual cash transactions above U.S. \$5,000 or combined monthly transactions above U.S. \$50,000 to be handled through the formal financial system, which is subject to the UIAF reporting requirements. It is illegal to transport more than the equivalent of US\$ 10,000 in cash across Colombian borders, and the GOC has criminalized cross-border cash smuggling and defined it as money laundering. In spite of improvements, customs officials are inadequately equipped to detect cross-border currency smuggling. Workers rotate frequently producing inadequately trained staff. In addition, the individual customs officials are held liable for any inspected article that they damage, causing hesitation in conducting thorough inspections. Reportedly, corruption is also a problem, and customs officials often lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes in this area.

In July 2007, the Drug Enforcement Administration (DEA) and the Department of Homeland Security’s Immigration and Customs Enforcement (ICE) agency seized approximately 20 million euros and U.S. dollars at the Miami International Airport belonging to several casas de cambio. Documents seized indicated that five of the ten registered Colombian casas de cambio had sent the currency to the United States with an ultimate destination of London. News reports in the Colombian press widely reported the downward effect on the black market currency exchange rate in Colombia resulting from these seizures. One of the five implicated financial institutions was Cambios y Capitales, which was designated by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) on October 10, 2007, as one of seven individuals and 14 companies tied to Specially Designated Narcotics Trafficker Juan Carlos Ramirez Abadia (alias “Chupeta”). Chupeta was arrested in Brazil on July 3, 2007, and is awaiting extradition to the U.S.

Colombian law provides for both conviction-based and nonconviction based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. Law 793 of 2002 eliminates interlocutory appeals that prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, places obligations on claimants to demonstrate their legitimate interest in property, requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets. The amount of time for challenges is shorter and the focus is on the seized item (cash, jewelry, boat, etc.), placing more burdens on the accused to prove the item was acquired with legitimately obtained resources. Law 785 of 2002, the National Drug Directorate (DNE) has the authority to conduct interlocutory sales of seized assets and contract with entities for the management of assets. Law 785 also permits provisional use of seized assets prior to a final forfeiture order, including assets seized prior to the enactment of the law.

In spite of improvements to the GOC's asset forfeiture capabilities, a number of problems remain. Concerns about personal liability have discouraged official action in some cases, exceptions in proceedings can still cause cases to drag on for years, and the pace of final decisions remains slow compared to new seizures. Until this year, prosecutors had limited discretion on asset seizures and had to seize all assets associated with a case, including those of minimal value or those that clearly risk loss under state administration, such as livestock. However, in November 2007, the Attorney General approved pre-seizure guidelines, applicable to forfeitures nationwide, which will require an evaluation of an asset's worth prior to seizure, and made other significant changes to the manner in which seizures for forfeiture will be conducted. The guidelines were also approved by the DNE Director. With limited resources and only 45 staff dedicated to asset management, the DNE must rely on outside contractors to store or manage assets. The GOC has established priorities for the proceeds of disposed assets; however, DNE's management task will only be reduced when the pace of judicial decisions and disposals exceeds new seizures. In 2007, the DNE and the Fiscalía concluded their work with the U.S. Department of Justice to establish regulations and guidelines that would give Colombian prosecutors authority not to seize assets of limited value. These guidelines will also aid DNE in its task of managing the assets under its control.

The GOC pursues the seizure of assets obtained by drug traffickers through their illicit activities. For the last four years, the Sensitive Investigations Unit (SIU) of the Colombian National Police (CNP), in conjunction with U.S. law enforcement and the Colombian Fiscalía have been investigating the Cali and North Valle cartels' business empires, including the Rodriguez Orejuela brothers, the Grajales family, and Juan Carlos Ramirez Abadia ("Chupeta"). The Cali and Norte Valle cartels, as well as their leaders and associated businesses, are on the OFAC list of Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. The Executive Order imposes economic sanctions authorities to attack the financial empires built by Colombian narcotics traffickers.

Colombian and U.S. law enforcement agencies have cooperated in a series of investigations designed to identify and seize assets either purchased by money gained through illegal drug activity or assets used to launder drug proceeds. In August 2007, OFAC added dozens of businesses and front men tied to Chupeta's financial empire to its list of SDNTs. In September 2007, the Colombian National Police and Colombian Fiscalía seized 332 business entities and assets tied to Chupeta, which were valued at approximately U.S. \$400 million. These entities and assets included office buildings, a resort hotel, night clubs, and an amusement park. In October 2007, OFAC added additional businesses and front men tied to Chupeta's financial empire to its list of SDNTs. These joint actions to apply economic sanctions have affected the Colombian drug cartels' abilities to use many of the financial assets they derived from their narcotics trafficking activities and have assisted the Colombian government in creating cases to seize narcotics-related assets.

In 2007, several major investigations by DEA and the SIU of the Department of Administrative Security (DAS) resulted in arrests and seizures of major money laundering organizations operating between the countries. These included Operation Rock Salt, which resulted in 60 arrests for money

laundering in Italy and Colombia, and the seizure of \$39 million in business entities and assets in Colombia. An additional \$10 million was seized under Operation Plata Sucia, which led to the arrests of 28 money launderers in Colombia and the United States, and the seizure of \$5 million, 65 kilograms of heroin, and 60 kilograms of cocaine in the United States in 2006. Extradition requests to the United States are pending in many of the arrests for Operation Plata Sucia. In January 2007, the Colombian National Police in cooperation with the DEA recovered approximately \$80 million in primarily U.S. currency and gold on raids on houses used to stash drug proceeds. Reportedly, the total value is probably the most ever seized by law enforcement in a single operation anywhere in the world.

ICE has also worked closely with Colombian authorities. In 2002, ICE supported the CNP establishment of a financial investigative unit within the organization's intelligence and investigations unit (DIJIN). The DIJIN has successfully initiated investigations against money laundering organizations in Colombia as well as pursued leads received from on-going U.S. investigations which have resulted in significant arrests and seizures. These include Operation Goldmine, which targeted an organization utilizing textiles as a means to launder narcotics proceeds between the U.S. and Colombia. This investigation led to 32 indictments in the U.S. and the seizure of over \$9 million. The DIJIN also successfully targeted the money-laundering infrastructure of Norte Valle Cartel leader Luis Hernando Gomez Bustamante. Coordinating actions with ICE domestic and foreign offices lead to the arrest of high-level members of this organization, which have been extradited to the U.S. from Colombia and other countries, to include its leader.

ICE has also helped Colombia establish a Trade Transparency Unit (TTU) with the GOC to aggressively target trade-based money laundering organizations that facilitate the movement of criminal proceeds across borders. TTUs provide a mechanism for the GOC and the USG to identify existing vulnerabilities in both U.S. and foreign financial and trade systems, and to jointly work associated criminal investigations. Colombia's TTU is one of four established foreign TTUs, and includes members from the Directorate of Customs and Revenue (DIAN), UIAF, and DIJIN.

Terrorist financing is now an autonomous crime in Colombia. A new law entered into effect in 2007 which amended the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups, in accordance with the Financial Action Task Force of South America (GAFISUD) and Egmont Group recommendations. The new law allows the UIAF to receive STRs regarding terrorist financing, and freeze terrorists' assets immediately after their designation. In addition, banks are now held responsible for their client base and must immediately inform the UIAF of any accounts held by newly designated terrorists. Banks also have to screen new clients against the current list of designated terrorists before the banks are allowed to provide prospective clients with services. To fulfill increased monitoring requirements, the GOC increased the size of UIAF staff to 65 positions and authorized the creation of new subdivisions for Information Management and Legal Affairs.

Colombian law is unclear on the government's authority to block assets of individuals and entities on the UN 1267 Sanctions Committee consolidated list. The government circulates the list widely among financial sector participants, and banks are able to close accounts but not seize assets. Banks also monitor other lists, such as OFAC's publication of Specially Designated Terrorists. Charities and nongovernmental organizations (NGOs) are regulated to ensure compliance with Colombian law and to guard against their involvement in terrorist activity. This regulation consists of several layers of scrutiny, including the regulation of incorporation and the tracing of suspicious financial flows through the collection of intelligence or STR reporting.

The GOC is a member of GAFISUD. However, as a result of the GOC's failure to pay its membership dues dating back to 2004 (totaling approximately \$87,000), GAFISUD placed sanctions on Colombia in July and suspended its membership on December 1. According to GOC officials, legislation must be passed to authorize the GOC to pay its membership dues; past dues had been paid without legal

authorization. At its December plenary meeting, GAFISUD agreed to reinstate Colombia's membership, but the GOC's participation in GAFISUD-sponsored events is limited, and the GOC does not have a voice at GAFISUD plenary meetings. The GAFISUD Secretariat will send a letter to the President of Colombia outlining its concerns and a high-level delegation from various GAFISUD member countries will meet with GOC officials in 2008.

Colombia is a member the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. The UIAF is a member of the Egmont Group, and has signed memoranda of understanding with 27 FIUs around the world. The GOC is a party to the 1988 UN Drug Convention, the International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOC has signed, but not yet ratified, the Inter-American Convention against Terrorism.

In 2007, the Government of Colombia made additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The implementation of a formal terrorist finance law is another development in fighting terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. However, weaknesses remain. The growth in contraband trade to launder illicit drug proceeds will require even greater interagency cooperation within the GOC, including coordination between the UIAF and DIAN, the tax and customs authority. Congestion in the court system, procedural impediments and corruption remain problems. Limited resources for prosecutors, investigators, and the judiciary hamper their ability to close cases and dispose of seized assets. Further, streamlined procedures for the liquidation and sale of seized assets under state management could help provide funds available for Colombia's anti-money laundering and counter-terrorist financing regime. The GOC is also strongly encouraged to enact legislation to permit the use of proceeds from confiscated assets to support its law enforcement efforts. In addition, the GOC should ensure that the necessary legislation is passed to allow it to pay its GAFISUD dues and become active in GAFISUD once again.

Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. Comoros is not a principal financial center for the region. An anti-money laundering (AML) law, which addresses many of the primary AML issues of concern, was passed by Presidential Decree in 2004. However, Comoran authorities lack the capacity to effectively implement and enforce the legislation, especially on the island of Anjouan.

In May 2006, Muslim cleric Ahmed Abdallah Mohamed Sambi was elected President in the first peaceful and democratic transfer of power in Comoros' post-independence history. He won the election with 58 percent of the vote after campaigning on promises to fight corruption and unemployment. The presidency of the union rotates between the three islands. The former incumbent, Azali Assoumani, represented Grand Comore; Sambi is from Anjouan. The three islands in the Comoros continue to retain much of their autonomy, particularly with respect to their security services, economies, and banking sectors.

One year after Sambi's election, Island president (governor) elections were scheduled on Grande Comore, Moheli, and Anjouan. The first two held free and fair elections. In Anjouan, Colonel Bacar refused elections and de facto seceded from the Union. In October 2007, the African Union applied financial and travel sanctions on Bacar and his illegitimate government. Union President Sambi and his cabinet are unable to travel to, or govern, the island of Anjouan.

Union Vice President Idi Nadhoim hosted a seminar in early 2007 on policies to combat money laundering and terrorist finance. The event was sponsored by the World Bank and the Bank of France. Union Central Bank officials, commercial banks, and operators participated, with a focus on Union policies with regard to Anjouan's illicit banking license activities. Marc Lantieri, Head of the Franc Zone at the Bank of France, made a keynote presentation on financial risk management and money laundering.

At the same seminar, Vice President Nadhoim emphasized that a stable and healthy financial system was a prerequisite for economic development. Jean Pierre Michau, an advisor to the Governor of the Bank of France, stated firmly that the Anjouan government's Internet-based banking license sales were against Comoran law and facilitated fraudulent banking activity. Vice President Nadhoim publicly accused Mr. F. LeCler of La Réunion as an accomplice of Anjouan in setting up money laundering operations. The Vice President also said Mr. Ronnie Dvorkin of "Anjouan Corporate Services" based in London was accused of violating Union Laws in his dealings with Anjouan.

Soon thereafter, Central Bank Governor Abdoulbastoi sent the United States Embassy a comprehensive report on Union Government policies and actions with regard to illicit Anjouan banking activities. Citing the 2003 law that conferred sole authority for granting banking licenses on the Union Central Bank, the Governor reported he had informed financial authorities in France, Brussels, and the United States to prohibit all activities by Anjouan-registered entities. The Governor repeated an earlier request that U.S. or European authorities help the Comoros by closing down all websites associated with Anjouan, including National Bank of Anjouan, International Company Office, Wall Street Bank, anjouan.net, anjouan.com, anjouan.org and numerous others.

The Union Central Bank has for years corresponded with French commercial banking authorities to request action against Anjouan entities. The Union Government has also issued numerous public announcements warning the public against all Anjouan financial entities. A regularly-updated circular lists the six banks properly accredited by the Union Central Bank in the Comoros: Central Bank of Comoros, Commerce and Industry Bank, Comoros Development Bank, National Post Office and Financial Services Company, Meck Union, and Sanduk Union.

The 2004 federal-level AML law is based on the French model. The main features of the law are that it: requires financial and related records to be maintained for five years; permits assets generated or related to money laundering activities to be frozen, seized and forfeited; requires residents to declare all currency or financial instruments upon arrival and departure, and nonresidents to declare all financial instruments upon arrival and all financial instruments above Comoran francs 500,000 (approximately U.S. \$1,250) on departure; permits provision and receipt of mutual legal assistance with another jurisdiction where a reciprocity agreement is in existence and confidentiality of financial records is respected; requires nonbank financial institutions to meet the same customer identification standards and reporting requirements as banks; requires banks, casinos and money exchangers to report unusual and suspicious transactions (by amount or origin) to the Central Bank and prohibits cash transactions over Comorian francs 5 million (approximately U.S. \$12,500); and criminalizes the provision of material support to terrorists and terrorist organizations. Although there is a suspicious activity filing requirement in the Union's AML law, there does not appear to be an independent financial intelligence unit in either Anjouan or the Union. As of February 2006, no suspicious transaction reports had been filed with the Comorian Central Bank in Grand Comore as required under the existing Union law, and the branch of the Central Bank located in Anjouan had no knowledge of the shell bank entities that have been licensed by Anjouan's Offshore Finance Authority, which apparently operates independently from the Union's Central Bank and has licensed some 300 offshore banks, many of which appear to be shell banks.

Foreign remittances from Comorans abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorons. Until recently most remittances came

via informal channels, but in 2006 Western Union established a presence to capture part of this market.

Union authorities have limited ability to implement AML laws in Anjouan and Moheli. Similarly, the island governments of Anjouan and Moheli may have limited control over AML matters. Although Moheli has its own AML law in effect (the Anti-Money Laundering Act of 2002), the law itself has some serious shortcomings and authorities lack the resources and expertise to enforce its provisions. Comprehensive information on Anjouan's laws and regulations is difficult to obtain, but it appears Anjouan does have an AML law (the Money Laundering Prevention Act, Government Notice 008 of 2005) but reportedly the law applies to Anjouan and not to the offshore entities it licenses. Little is known about: (i) the procedures that have been established to review and approve offshore licenses issued before the enactment of the AML law; (ii) the procedures that have been established to review and approve ongoing bank license applications and to supervise and monitor institutions for compliance with Anjouan laws; and (iii) the efforts and resources available to implement these procedures and enforce compliance.

President Sambi has reiterated Union Government support for efforts made under former President Azali to bring AML enforcement under Union government jurisdiction. All banking and financial institutions operating within the jurisdiction of the Union of the Comoros, whether offshore or onshore, must abide by the provisions of legislation No. 80-7 of May 3, 1980. According to article 7 of this legislation, a bank or any other financial institution cannot operate in the Union of the Comoros without prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Thus, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Union Finance Minister contravene the May 3, 1980 legislation. Since taking office, President Sambi has sought to have corrupt former officials prosecuted. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit Sambi. Throughout 2006 there were reports that Sambi's authority in Anjouan is limited. There are reports that high-ranking Comoran officials tolerate and possibly benefit from money laundering. The lack of political will is exacerbated by the lack of capacity. Under the Constitution, the Union AML applies to all three islands, but is not enforced in Anjouan.

While the Comoros is not a principal financial center for the region, Moheli and Anjouan may have attempted or may be attempting to develop an offshore financial services sector as a means to finance government expenditures. The Anjouan island government's claim that unrelated companies are presenting themselves as licensed by the government of Anjouan makes authoritative information on Anjouan's offshore sector difficult to establish. Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, license off-shore banks. Together, the islands have licensed more than 300 banks. Applicants for banking licenses in either jurisdiction are not required to appear in person to obtain their licenses. In Anjouan, only two documents (a copy of the applicant's passport and a certificate from a local police department certifying the lack of a criminal record) are required to obtain an offshore license and fax copies of these documents are acceptable. Even if additional information was to be required, it is doubtful that either jurisdiction has the ability or resources to authenticate and verify the information. Neither jurisdiction is capable, in terms of expertise or resources, of effectively regulating an offshore banking center. Anjouan, and probably Moheli as well, has delegated much of its authority to operate and regulate the offshore business to private, nonComoran domiciled parties. In November 2004 and again in December 2005, Anjouan island government officials denied island government involvement in the offshore sector. They said the Union of the Comoros Central Bank was the only authority for the offshore banking sector in the country and insisted the Anjouan island government had not established its own central bank. They admitted that several years earlier the government of Anjouan considered starting an offshore banking sector, but they had not pursued it. Substantial concern remains that Anjouan, and possibly Moheli, allows shell banking activity. Union President Sambi has repeatedly

requested international assistance in closing any shell banks or illicit financial entities that operate within the Comoros without legitimate approval.

France, the former colonial power, maintains substantial influence and activity in Comoros, and has bypassed the Union and island governments to, where possible, prosecute suspects in money laundering or shell banks under French law. Although Comoros lacks homegrown narcotics, the islands are used as a transit site for drugs coming mainly from Madagascar. In view of international concern about drug trafficking, in 1993 France began providing technical expertise in this field to Comoros.

In addition to offshore banks, both Moheli, pursuant to the International Companies Act of 2001, and Anjouan, pursuant to Ordinance Number 1 of 1 March 1999, license insurance companies, Internet casinos, and international business companies (IBC's). Moheli claims to have licensed over 1200 IBC's. Bearer shares of IBC's are permitted under Moheli law. Anjouan also forms trusts, and registers aircraft and ships (without requiring an inspection of the aircraft or ship in Anjouan).

Comoros is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

Comoros has become the 12th member of the free-trade area of the Common Market for Eastern and Southern Africa (Comesa). The U.S. Export-Import Bank (ExIm Bank) has added Comoros to its Short-Term Insurance Pilot Program for Africa (STIPP), while renewing the program for three years, beginning March 31, 2006.

The Government of the Union of the Comoros (GOC) should harmonize anti-money legislation for the three islands that comprise the federal entity. The legislation should adhere to world standards. A unified financial intelligence unit should be established and the unregulated offshore financial sectors in Moheli and Anjouan should either be regulated by federal authorities or be shut down. In either case, bearer shares should be prohibited. The list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list should be circulated to banks in the Comoros. The deficiencies in the anti-money laundering/terrorist financing regimes in the Comoros and the inability to implement existing legislation make it vulnerable to traditional money laundering and to the financing of terrorism. Comoros should make every effort to comport to international standards. The total annual operating budget of the Union Finance Ministry is less than U.S. \$100,000. Combined with the lack of political strength, it is highly unlikely that the needed reforms in Moheli and Anjouan will be successfully implemented without significant outside assistance.

Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. Cook Islanders are citizens of New Zealand. The Cook Islands' offshore sector makes it vulnerable to money laundering. The sector offers banking, insurance, international trusts, and formation of international business companies and trusts. However, due to recent legislative and regulatory changes, the Cook Islands complies with current international standards.

The domestic banking system is comprised of branches of two major Australian banks and the local Bank of the Cook Islands (BCI). Domestic banks are primarily involved in traditional deposit taking and lending. The BCI operates as a stand-alone institution competing against the two Australian banks and is no longer engaged in development lending. Legislation allows for development lending to be undertaken in the future by a separate company not subject to supervision by the Financial Supervisory Commission (FSC). In addition, nonperforming loans made by the Cook Islands Development Bank have been transferred to another affiliated company. In addition to the three

domestic banks, the Cook Islands financial sector also consists of four international banks, seven trustee companies, and six offshore and three domestic insurance companies. The domestic insurance companies are not regulated by the FSC, but legislation is being drafted to allow regulation to take place in 2008.

The Cook Islands has an offshore financial sector that licenses international banks and offshore insurance companies and registers international business companies (IBCs). The offshore sector also consists of company services and trusts, including asset protection trusts (APTs). APTs protect the assets of individuals from civil judgments in their home countries and are able to contain a “flee clause.” One of the purposes of a “flee clause,” is to evade law enforcement. If a foreign law enforcement agency makes an inquiry regarding the trust, the trust will be transferred automatically to another offshore center. According to officials of the Government of the Cook Islands (GOCI), the “flee clause” exists to transfer APTs in times of emergency, such as a natural disaster, but they may also incorporate clauses designed to avoid the courts of the jurisdiction they are in or investigations by regulatory authorities. In practice they are rarely used as they are difficult to implement without the trustee finding itself in breach of the law.

The Cook Islands was placed on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) in 2000. After the GOCI addressed deficiencies in its anti-money laundering regime by enacting legislative reforms, the FATF removed the Cook Islands from its NCCT list in February 2005. The FATF conducted a year-long monitoring program, which concluded in June 2006, to closely monitor the islands.

The Banking Act 2003 and the Financial Supervisory Commission Act (FSCA) 2004 established a new framework for licensing and prudential supervision of domestic and offshore financial institutions in the Cook Islands. The legislation requires international offshore banks to have a physical presence in the Cook Islands, transparent financial statements, and adequate records prepared in accordance with consistent accounting systems. The physical presence requirement is intended to prohibit shell banks. All banks are subject to a vigorous and comprehensive regulatory process, including on-site examinations and supervision of activities.

The FSCA established the Financial Supervisory Commission as the licensed financial sector’s sole regulator. The FSC is empowered to license, regulate, and supervise the business of banking. It serves as the administrator of the legislation that regulates the offshore financial sector. The FSC can license international banks and offshore insurance companies and register international companies. It also supervises trust and company service providers. Its policy is to respond to requests from overseas counterparts to the utmost extent possible. The FSC has taken a broad interpretation of the concept of “counterpart” and does not need to establish general equivalence of function before being able to cooperate.

Licensing requirements, as set out in the legislation, are comprehensive. The Banking Act 2003 and a Prudential Statement on Licensing issued in February 2004 contain detailed licensing criteria for both locally incorporated and foreign banks, including “fit and proper” criteria for shareholders and officers, satisfactory risk management, accounting and management control systems, and minimum capital requirements. The Banking Act 2003 defines banking business, prohibits the unauthorized use of the word “bank” in a company name, and requires prior approval for changes in significant shareholding.

By enacting the Financial Transactions Reporting Act (FTRA) 2003, which replaced a similar Act passed a year earlier, the Cook Islands authorities strengthened its anti-money laundering and counter-terrorist financing (AML/CTF) legal and institutional framework. Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The Financial Supervisory Commission (FSC), regulator of the licensed financial sector is drafting new insurance legislation. The legislation

will regulate the small domestic insurance sector and update supervision of the offshore insurance sector. Insurance intermediaries will also be regulated under the proposed legislation.

The FTRA imposes certain reporting obligations on 26 different types of institutions, including banks, offshore banking businesses, offshore insurance businesses, casinos, gambling services, insurers, financial advisors, solicitors/attorneys, accountants, financial regulators, lotteries and money remitters. The Minister of Finance can extend the reporting obligation to other businesses when required. Reporting institutions are required to retain all records related to the opening of accounts and financial transactions for a minimum of six years. The records must include sufficient documentary evidence to verify the customer's identity. In addition, reporting institutions are required to develop and apply internal policies, procedures, and controls to combat money laundering and to develop audit functions to evaluate such policies, procedures, and controls. Reporting institutions must comply with any guidelines and training requirements issued under the FTRA, as amended, and must provide internal training on all anti-money laundering matters. The FTRA provides for administrative and financial sanctions on institutions for noncompliance.

The FTRA requires the FSC to assess the compliance by licensed financial institutions with customer due diligence and record keeping requirements. Resulting reports and documentation from annual inspections are provided to the Cook Islands Financial Intelligence Unit (CIFIU). The CIFIU is also responsible for assessing compliance by nonlicensed institutions.

The CIFIU is the central unit responsible for processing disclosures of financial information in accordance with anti-money laundering and antiterrorist financing legislation. It became fully operational with the assistance of a Government of New Zealand technical advisor. The FTRA grants supervisory authority to the CIFIU, allowing it to cooperate with other regulators and supervisors, require reporting institutions to supplement reports, and obtain information from any law enforcement agency and supervisory body.

Obligated institutions are required to report any attempted or completed large currency transactions and suspicious transactions to the CIFIU. The currency reporting requirements apply to all currency transactions of NZ \$10,000 (approximately U.S. \$6870) and above, electronic funds transfers of NZ\$10,000 and above, and transfers of currency in excess of NZ \$10,000 into and out of the Cook Islands. Failure to declare such transactions could incur penalties. The CIFIU is required to destroy a suspicious transaction report if there has been no activity or information related to the report or to a person named in the report for six years. The CIFIU does not have an investigative mandate. If it determines that a money laundering offense, serious offense or terrorist financing offense has been or is being committed, it must refer the matter to law enforcement for investigation. The Minister of Finance, who is responsible for administrative oversight, appoints the head of the CIFIU.

The CIFIU is participating in the Pacific FIU database project (PFIUDP) provided by AUSTRAC, the Australian FIU. The CIFIU received a prototype of the database and is now testing the reporting and analysis capacity. The Pacific FIU Database Project includes other jurisdictions that will receive versions of the same database framework.

Since June 2004 the Cook Islands had made further progress in implementing its AML/CTF regime. The head of the CIFIU chairs the Coordinating Committee of Agencies and Ministries, which promotes, formalizes and maintains coordination among relevant government agencies; assists the GOCI in the formulation of policies related to AML/CTF issues; and enables government agencies to share information and training resources gathered from their regional and international networks. The AML/CTF consultative group of stakeholders facilitates consultation between government and the private sector, and ensures all financial sector players are involved in the decision making and problem solving process regarding AML/CTF regulations and reporting. The CIFIU is also a member of the Anti-Corruption Committee, along with the Office of the Prime Minister, Police, Crown Law, Audit Office, and the Financial Secretary.

The Terrorism Suppression Act 2004, based on the model law drafted by an expert group established under the auspices of the Pacific Islands Forum Secretariat, criminalizes the commission and financing of terrorism. The United Nations (Security Council Resolutions) Act 2003 allows the Cook Islands, by way of regulations, to give effect to the Security Council resolutions concerning international peace and security.

The GOCI is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The Cook Islands is an active member of the Asia/Pacific Group on Money Laundering (APG), an associate member of the FATF. The CIFIU became a member of the Egmont Group in June 2004, has bilateral agreements allowing the exchange of financial intelligence with Australia, and is negotiating a memorandum of understanding (MOU) with Thailand. The Cook Islands plans to become a member of the Offshore Group of Banking Supervisors (OGBS), once it has qualified by undergoing further evaluation. The GOCI is also an active member of the Association of Financial Supervisors of Pacific Countries and draws on the resources of this association and Pacific Financial Technical Assistance Centre for capacity building for FSC staff. The Cook Islands has received nine requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Five have been answered, and four are pending. The Cook Islands has not received any extradition requests from foreign countries, but successfully extradited one person from New Zealand.

The Cook Islands should continue to implement legislation designed to strengthen its nascent AML/CTF institutions. The Government of the Cook Islands should maintain vigilant regulation of its offshore financial sector, including its asset protection trusts, to ensure that its offshore sector comports with international standards.

Costa Rica

Although Costa Rica is not a major regional financial center, it remains vulnerable to money laundering and other financial crimes. Narcotics trafficking (mainly cocaine) continues to be a primary motive for money laundering, but fraud, trafficking in persons, arms trafficking, corruption, and the presence of Internet gaming companies all contribute to money laundering activity. While local criminals are active, the majority of criminal proceeds laundered derive primarily from foreign criminal activity. Reforms in 2002 to the Costa Rican counternarcotics law expanded the scope of anti-money laundering regulations, but also, unintentionally, created an opportunity to launder funds by eliminating the government's licensing and supervision of casinos, jewelers, realtors, attorneys, cash couriers, and other nonbank financial institutions. While these loopholes have not yet been closed, these weaknesses should be addressed as part of a legal reform bill on money laundering that may be passed in 2008. Bank fraud and counterfeit currency, though they do exist, do not seem to be on the rise.

Gambling is legal in Costa Rica, and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. There are well over 250 sports-book companies registered to operate in Costa Rica. One U.S. citizen, who had been running a sports-book company in Costa Rica, was arrested in the Dominican Republic in 2007.

Costa Rica is not considered an offshore financial center. While the formal banking industry in Costa Rica is tightly regulated, the offshore banking sector, which offers banking, corporate and trust formation services, remains an area of concern. Foreign-domiciled offshore banks can only conduct transactions under a service contract with a domestic bank, and they do not engage directly in financial operations in Costa Rica. They must also have a license to operate in their country of origin. Furthermore, they must comply with Article 126 of the Costa Rican Central Bank's Organic Law, which requires offshore banks to have assets of at least U.S. \$3 million, a physical presence in Costa Rica, and be subject to supervision by the banking authorities of their registered country. Shell banks

are not allowed in Costa Rica and regulated institutions are forbidden from having any direct or indirect relationships with institutions that may be described as shell banks or fictitious banks. Bearer shares are not permitted in Costa Rica.

Currently, six offshore banks maintain correspondent operations in Costa Rica: three from The Bahamas and three from Panama. The Government of Costa Rica (GOCR) has supervision agreements with its counterparts in both countries, permitting the review of correspondent banking operations. However, these counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In 2005, the Attorney General ruled that the Superintendent General of Financial Entities (SUGEF) lacked authority to regulate offshore operations due to an apparent contradiction between the 1995 Organic Law of the Costa Rican Central Bank and Law 8204. Draft legislation to correct the contradiction and reassert the SUGEF's regulatory power is under review in the Legislative Assembly and is expected to pass in 2008. Costa Rican authorities acknowledge that they are currently unable to adequately assess risk.

The GOCR reports that Costa Rica is primarily used as a bridge to send funds to and from other jurisdictions using, in many cases, companies or established banks in offshore financial centers. Alternative remittance systems exist in Costa Rica, mainly as a result of Costa Rican immigration to the United States, or Nicaraguans to Costa Rica. However, there is no confirmation that these remittance systems are used for money laundering.

There are 287 free trade zones (FTZs) within Costa Rica. The Promotora del Comercio Exterior de Costa Rica (PROCOMER) manages the FTZ regime and has responsibility for registering all qualifying companies. PROCOMER's qualification process consists of conducting due diligence on a candidate company's finances and assessing the total cost of ownership. PROCOMER annually audits all of the firms within the FTZ regime and touts its system of tight controls. The four major types of firms operating in Costa Rica's FTZ regime are manufacturing, services, trading, and administrative organizations. PROCOMER reports that there has been no evidence of money laundering activity in the FTZs in 2007.

In 2002, the GOCR enacted Law 8204. Law 8204 criminalizes the laundering of proceeds from all serious crimes (not only drug-related money laundering), which are defined as crimes carrying a sentence of four years or more. Law 8204 obligates financial institutions and other businesses to identify their clients, report currency transactions over U.S. \$10,000 and suspicious transactions to the financial intelligence unit (FIU), the Unidad de Analisis Financiero (UAF). Law 8204 also requires that financial records be retained for at least five years, and that the beneficial owners of accounts and funds involved in transactions be identified. While Law 8204, in theory, applies to the movement of all capital, current regulations are narrowly interpreted so that the law applies only to those entities that are involved in the transfer of funds as a primary business purpose, such as exchange houses and stock brokerages. Therefore, the law does not cover such entities as casinos, dealers in jewels and precious metals, insurance companies, intermediaries such as lawyers, accountants or broker/dealers, or Internet gambling operations, as their primary business is not the transfer of funds.

Costa Rican financial institutions are regulated by the Office of the Superintendent General of Financial Entities (SUGEF), the Superintendent General of Securities (SUGEVAL), and the Superintendent of Pensions (SUPEN). All three of these entities fall under the National Council of Supervision of the Financial System (CONASSIF). All financial entities subject to the jurisdiction of SUGEF, SUGEVAL and SUPEN are obligated to submit suspicious transaction reports (STRs), regardless of the amount involved or transaction reported. Law 8204 does not establish any protection for reporting individuals with respect to their cooperation with law enforcement entities. Nevertheless, this does not exempt them from reporting; if they do not file STRs, they may be subject to pecuniary sanctions established in Article 81 of Law 8204.

The UAF, which is located within the Costa Rican Drug Institute (ICD), became operational in 1998. Article 123 of Law 8204 empowers the UAF to request, collect and analyze STRs and cash transaction reports (CTRs) submitted by obligated entities. The Money Laundering, Financial, and Economic Crimes Unit of the Judicial Investigative Organization (OIJ), under the Public Ministry (Prosecutor's Office), receives a copy of the information sent to the UAF. This practice gives rise to the possibility of duplication of information and waste of time and resources, and the risk of contamination or leakage of information. Each superintendence holds the CTRs until the UAF requests them. All requests and reports from the UAF must be signed by the Director of the ICD. Approval and authorization is therefore given by the Director of the ICD, not the Director of the UAF. This practice may interfere with the UAF's operational autonomy.

The UAF has no regulatory responsibilities. The UAF has access to the records and databases of financial institutions and other government entities, but must obtain a court order if the information collected is to be used as evidence in court. Additionally, there are formal mechanisms in place to share information domestically and with other countries' FIUs.

In spite of its broad access to government information and high levels of cooperation with the financial sector, the UAF remains ill-equipped and under-funded to provide information needed by investigators. Additionally, in 2007, the UAF had a 40 percent turnover in personnel, including one of their most senior analysts. Nevertheless, in 2007, the UAF continued to increase the quality of its analysis and forwarded more thoroughly analyzed cases to prosecutors. The UAF received 280 STRs in 2007, 92 of which are still under review.

The GOCR body responsible for investigating financial crimes is the OIJ. The OIJ is assisted by the UAF and has adequately trained staff. In 2007, there were two prosecutions for financial crimes.

All persons carrying entering or exiting Costa Rica are required to declare any amount over U.S. \$10,000 to Costa Rican officials at ports of entry. Declaration forms are required. Cash smuggling reports are entered into a database maintained by ICD and is shared with appropriate government agencies, including the UAF.

Articles 33 and 34 of Law 8204 cover asset forfeiture and stipulate that all movable or immovable property used in the commission of crimes covered by this act shall be subject to preventative seizure. When seizure or freezing takes place, the property is placed in a legal deposit under the control of ICD. The banking industry closely cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. During 2007, officials seized over U.S. \$9.6 million (an increase over the U.S. \$5.2 million seized in 2006) in narcotics-related assets, much of it in undeclared cash. Seized assets are processed by the ICD and if judicially forfeited, are divided among drug treatment agencies (60 percent), law enforcement agencies (30 percent), and the ICD (10 percent).

Although the GOCR has ratified the major UN counterterrorism conventions, terrorist financing is not a crime in Costa Rica. In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions. The draft law, when passed, would expand existing conspiracy laws to include the financing of terrorism and enhance existing narcotics laws by incorporating the prevention of terrorist financing into the mandate of the ICD. In 2007, Costa Rica was notified that if its terrorist financing law was not passed by May 2008, it risks being expelled from the Egmont Group of financial intelligence units. The GOCR expects the legislation to be passed by the May 2008 deadline.

Costa Rican authorities receive and circulate to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. However, these authorities cannot block, seize, or freeze property without prior judicial

approval. Thus, Costa Rica lacks the ability to expeditiously freeze assets connected to terrorism. No assets related to designated individuals or entities were identified in Costa Rica in 2007.

Costa Rica fully cooperates with appropriate USG law enforcement agencies and other governments investigating financial crimes related to narcotics and other crimes. Articles 30 and 31 of Law 8204 grant authority to the UAF to cooperate with other countries in investigations, proceedings, and operations concerning financial and other crimes covered under that law.

Costa Rica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On March 21, 2007, the GOCR ratified the UN Convention against Corruption. The GOCR has also signed, but not yet ratified, the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, and has ratified the Inter-American Convention against Terrorism. Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF), and assumed the CFATF presidency in 2007. The most recent mutual evaluation of Costa Rica was conducted by the CFATF in July 2006. The GOCR is a member of the Money Laundering Experts Working Group of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD). The UAF is a member of the Egmont Group.

Even though the Government of Costa Rica convicted a handful of individuals for money laundering over the last several years, further efforts are required to bring Costa Rica into compliance with international anti-money laundering and counter-terrorist financing standards. The GOCR should criminalize terrorist financing prior to the Egmont Group deadline for expulsion. The GOCR should also pass legislation that reconciles contradictions regarding the supervision of its offshore banking sector, and should extend its anti-money laundering legislation and regulations to cover the Internet gaming sector, dealers in jewelry and precious metals, attorneys, casinos, and other nonbank financial institutions. Costa Rica should ensure that its financial intelligence unit and other GOCR authorities are adequately equipped to combat financial crime.

Côte d'Ivoire

The Republic of Cote d'Ivoire is an important West African regional financial hub. Money laundering and terrorist financing in Cote d'Ivoire are not primarily related to narcotics proceeds. Criminal proceeds that are laundered are reportedly derived from regional criminal activity, such as the smuggling of consumer goods and agricultural products. Reportedly, most of the smuggling networks are organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. Due to the ongoing political and economic turmoil in Cote d'Ivoire, respect for the rule of law continues to deteriorate. As a result, Ivorian and some other West African nationals are becoming more and more involved in criminal activities and the subsequent laundering of funds. Cote d'Ivoire is ranked 150 out of 179 countries in Transparency International's 2007 Corruption Perceptions Index. The extent to which Ivorian territory is used in the growing use of West Africa as a transshipment point for drugs from South America to Europe is largely unknown. The de facto ongoing division of the country makes such an assessment, as well as that of Cote d'Ivoire's possible associated role as a drug laundering center, difficult.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, including cocoa, timber, textiles, tobacco products, and light motorcycles. There have also been reports of an increase in the processing and smuggling of diamonds from mines located in the north. Ivorian law enforcement authorities have, until the mid-2007, had very little control over the northern half of the country. While national authority is slowly being redeployed, the government's control over borders in the formerly rebel-controlled regions of the country remains very weak. The relationship between revenues associated with smuggled goods and narcotics proceeds remains unclear due to the lack of effective border controls in the north. Smuggling of sugar, cotton, cocoa, cars, and

pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of taxes. According to the Office of the Customs Financial Enquiries, the cross-border trade of diamond and cocoa over Cote d'Ivoire's porous borders generates contraband funds that are laundered into the banking system via informal moneychangers. Criminal enterprises use both the formal and informal financial sector to launder funds. Cash is moved both via the formal banking sector and by cash couriers. Cash earned by immigrant or migrant workers generally flows out of Cote d'Ivoire, going to extended families outside the region.

Banks have begun to resume operations, but because banking services were largely absent from the northern part of Côte d'Ivoire until the end of 2007, informal money couriers, money transfer organizations similar to hawaladars and, increasingly, goods transportation companies transferred funds domestically, as well as within the sub-region. Domestic informal value transfer systems are not regulated. Informal remittance transfers from outside Cote d'Ivoire violate West African Central Bank (BCEAO) money transfer regulations. The standard fee for informal money transfer services is approximately ten percent. In addition to transferring funds, criminal enterprises have been known to launder illicit funds by investing in real estate and consumer goods such as used cars in an effort to conceal the source of funding.

Hizballah is present in Côte d'Ivoire and conducts fundraising activities, mostly among the large Lebanese expatriate community. The Ivorian government has taken no legal action to prevent the misuse of charitable and or other nonprofit entities that can be used as conduits for the financing of terrorism. Reportedly, the Ministry of Interior Security is addressing this problem.

There are no free trade zones in Cote d'Ivoire. In August 2004, the Ivorian government adopted a plan for the creation of a free trade zone for information technology and for biotechnology. This project remains dormant.

The Economic and Financial Police report an ongoing rise in financial crimes related to credit card theft and foreign bank account fraud, which includes wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet based advance fee scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud, by merchants. The country has the largest bank network in the region. French financial interests account for the majority of retail and other banking and insurance services. The banking law was recently changed to require banks be capitalized with U.S. \$10 million and nonbank financial institutions (mortgage firms, insurance companies, etc.) with U.S. \$5 million.

The Ivorian banking law, enacted in 1990, prevents disclosure of client and ownership information, but does allow the banks to provide information to judicial authorities such as investigative magistrates. The law also permits the use of client and ownership information as evidence in legal proceedings or during criminal investigations. The Tax and Economic police can request information from the banks.

Until recently, the penal code criminalized only money laundering related to drug trafficking, fraud, and arms trafficking. On November 29, 2005, the National Assembly adopted the l'Union Economique et Monetaire Ouest Africaine/West African Economic and Monetary Union (l'UEMOA/WAEMU), common law on money laundering, making all forms of money laundering a criminal offense.

The law focuses on the prevention of money laundering and also expands the definition to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It includes standard "know your customer" requirements for banks and other financial institutions, and establishes procedures and a suspicious transaction reporting obligation which covered institutions must follow to assist in the detection of money laundering. The law provides for the creation of an Ivorian financial intelligence unit (FIU), as well as a legal basis for international cooperation. The new law includes

both criminal and civil penalties, and permits the freezing and seizure of assets, which can be instruments for and proceeds of crime. Legitimate businesses are among the assets which can be seized if used to launder money or support terrorist or other illegal activities. Substitute assets cannot be seized if there is no relationship with the offense.

The money laundering law provides for the establishment of a financial intelligence unit (FIU) known as “Cellule Nationale de Traitement des Informations Financieres” (CENTIF). Participants at the September 2007 L’UEMOA/WAEMU meeting of finance ministers had urged Cote d’Ivoire to accelerate the start of CENTIF operations. CENTIF members were nominated on December 20, 2007. The government of Cote d’Ivoire announced on January 8, 2008 that CENTIF is now operational, and its members were sworn in on January 16, 2008. It reports to the Finance Minister. On a reciprocal basis and with the permission of the Ministry of Finance, CENTIF can share information with other FIUs in L’UEMOA/WAEMU and with those of nonL’UEMOA/WAEMU countries, as long as those institutions keep the information confidential.

Once established, the FIU will continue to work with previously established investigative units such as the Centre de Recherche Financiere (CRF) at the Department of Customs and the Agence Nationale de Strategie et d’Intelligence (ANSI) at the presidency. The CRF and the ANSI will still continue their missions, which include fiscal and customs fraud and counterfeiting. The Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance, the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing.

The Ministry of Finance, the BCEAO, and the West African Banking Commission, headquartered in Cote d’Ivoire, supervise and examine compliance with anti-money laundering/counter-terrorist financing (AML/CTF) laws and regulations. All Ivorian financial institutions are required to maintain customer identification and transaction records for ten years. Additionally, as in all BCEAO member countries, all bank deposits over CFA 5,000,000 (approximately U.S. \$10,000) must be reported to the BCEAO, along with customer identification information. Law enforcement authorities can request access to these records to investigate financial crimes through a public prosecutor. In 2007, there were no arrests or prosecutions for money laundering or terrorist financing.

The new legislation imposes a ten-year retention requirement on financial institutions to retain records of all “significant transactions,” which are transactions with a minimum value of CFA 50,000,000 (approximately U.S. \$100,000) for known customers. New money laundering controls apply to nonbank financial institutions such as exchange houses, stock brokerage firms, insurance companies, casinos, cash couriers, national lotteries, nongovernment organizations, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The law also imposes certain customer identification and record maintenance requirements on casinos and exchange houses. The tax office (Ministry of Finance) supervises these entities. All Ivorian financial institutions, nonfinancial businesses, and professions subject to the scope of the money laundering law are required to report suspicious transactions. The Ivorian banking code protects reporting individuals. Their identities are not divulged with respect to cooperation with law enforcement authorities.

Cote d’Ivoire monitors and limits the international transport of currency and monetary instruments under L’UEMOA/WAEMU administrative regulation R/09/98/CM/L’UEMOA/WAEMU. There is no separate domestic law or regulation. When traveling to another L’UEMOA/WAEMU country, Ivorian and expatriate residents must declare the amount of currency being carried out of the country. When traveling to a destination other than another L’UEMOA/WAEMU country, Ivorian and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately U.S. \$1,000) for tourists, and two million CFA francs (approximately U.S. \$4,000) for business operators, without prior approval from the Department of External Finance of the

Ministry of Economy and Finance. If additional amounts are approved, they must be in the form of travelers' checks.

Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSCR 1373, although financing of all "serious crimes" falls under the domain of the law. Until the passage of the 2005 money laundering law, the Government of Cote d'Ivoire (GOCI) relied on several L'UEMOA/WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the GOCI to implement the asset freeze provisions of UNSCR 1373. The BCEAO and the government report that they promptly circulate to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's Consolidated List and those on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. To date, no assets related to terrorist entities or individuals have been discovered, frozen or seized.

The GOCI participates in the Intergovernmental Group for Action against Money Laundering (GIABA) based in Dakar, which is the Financial Action Task Force-style regional body (FSRB) for West Africa. GIABA has scheduled a mutual evaluation scheduled for Cote d'Ivoire for November 2008. Other than the authority granted to CENTIF by the AML law, the GOCI has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with United States on money laundering and terrorist financing.

Cote d'Ivoire has demonstrated a willingness to cooperate with the United States in investigating financial or other crimes. For example, in a 2007 case, a prominent American government official based in the UK was defrauded by a party based in Cote d'Ivoire who was using the individual's credit card information to purchase expensive medical equipment and ship it to Cote d'Ivoire. While the perpetrator(s) were not apprehended, Ivorian authorities worked cooperatively with U.S. law enforcement.

Cote d'Ivoire is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. The GOCI has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The Government of Cote d'Ivoire should specifically criminalize terrorist financing and become a party to the relevant UN Conventions. The Ministry of Finance should work to build capacity at CENTIF to maximize effectiveness in FIU functions, especially analysis, outreach and information sharing. CENTIF should work toward becoming a member of the Egmont Group. The GOCI's law enforcement and customs authorities need to implement measures to diminish smuggling, trade-based money laundering and informal value transfer systems. The GOCI should also enact legislation criminalizing terrorist financing and facilitating information sharing with other countries. Authorities should also take steps to halt the spread of corruption that permeates both commerce and government and facilitates the continued growth of the underground economy and money laundering. Cote d'Ivoire should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following an unsuccessful coup d'etat directed from Greece. Since then, the Republic of Cyprus (ROC) has controlled the southern two-thirds of the country, while a Turkish Cypriot administration calling itself the "Turkish Republic of Northern Cyprus (TRNC)" controls the northern part. Only Turkey recognizes the "TRNC." The U.S. Government recognizes only the Republic of Cyprus. This report primarily discusses the area controlled by the ROC but also includes a separate section on the area administered by Turkish Cypriots.

Cyprus is a major regional financial center with a robust financial services industry and a significant amount of nonresident businesses. As with all such centers, Cyprus remains vulnerable to international money laundering activities. Fraud along with other financial crimes and narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus.

A number of factors have contributed to the development of Cyprus as a financial center: the island's central location; a preferential tax regime, double tax treaties with 40 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations); a labor force well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and EU membership.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks and money transfer businesses; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission. Three entities act as regulators for designated nonfinancial businesses and professions (DNFBPs): the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the financial intelligence unit (FIU) supervises real estate agents and dealers in precious metals and stones. The supervisory authorities may impose administrative sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus' anti-money laundering (AML) laws and regulations.

Cyprus currently hosts a total of 43 banks, 17 of which are incorporated locally. The remaining 26 banks are branches of foreign-incorporated banks and conduct their operations mainly with nonresidents. At the end of August 2007, the cumulative assets of all banks were U.S. \$112 billion. Under the EU's "single passport" policy, banks licensed by competent authorities in EU countries could establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus. By the end of 2007, nine foreign banks were operating a branch in Cyprus under this arrangement.

Cyprus hosts seven licensed money transfer companies, 65 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 40 licensed insurance companies, 400 licensed real estate agents, 2,311 registered accountants, 1,810 practicing lawyers, and around 165 cooperative credit institutions, controlling about 32 percent of total deposits. Stricter EU requirements on credit institutions have pushed cooperative credit institutions to merge on a large scale over the last three years. Their number shrank from 359 to the current 165 in less than three years, and authorities expect it to drop to just over 100 by the middle of 2008.

In recent years, Cyprus has introduced tax and legislative changes effectively abolishing all legal and substantive distinctions between domestic and offshore companies. All Cypriot companies now pay taxes at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. Cyprus has lifted the prohibition from doing business domestically and companies formerly classified as offshore are now free to engage in business locally. In March 2007, Cyprus withdrew from the Offshore Group of Banking Supervisors. The Cypriot government made this move specifically to change the focus and impression of its foreign business from "offshore" to "international." By removing any distinction between resident and nonresident or on-shore and offshore companies, the same disclosure, reporting, tax and other laws and regulations apply equally to all registered companies. Despite these stricter standards, few of the estimated 54,000 nonresident companies established in Cyprus as of 2006 have taken themselves off the company register and the number of new nonresident companies registering in Cyprus continues to increase as a result of the low tax rate and high service quality.

Cyprus continues to revise its anti-money laundering (AML) framework to meet evolving international standards. The Prevention and Suppression of Money Laundering Activities Law criminalizes all

money laundering, establishes a customer identification requirement and obligations for suspicious transaction reporting, provides for the confiscation of proceeds from serious crimes, and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take. The AML law establishes the financial intelligence unit (FIU) and authorizes criminal (but not civil) seizure and forfeiture of assets. The definition of predicate offense is any criminal offense punishable by a prison term exceeding one year. Cypriot AML legislation addresses government corruption, provides for the sharing of assets with other governments, and facilitates the exchange of financial information with other FIUs. Cypriot authorities reportedly have full access to information concerning the beneficial owners of every company registered in Cyprus. This includes companies doing business abroad and companies with foreign beneficial owners and shareholders. Due diligence and reporting requirements extend to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems. Although the professional organizations for accountants and lawyers publicize strict “know your customer” regulations, the regulatory oversight of these sectors is reportedly nearly nonexistent. Violations result in administrative fines of up to Cyprus Pounds (CP) 3,000 (approximately U.S. \$7,500). The FIU can instruct banks, financial institutions and other obligated entities to delay or prevent execution of customers’ transactions. Casinos and Internet gaming sites are not permitted, although sports betting halls are allowed.

ROC law requires all persons entering or leaving Cyprus to declare all currency, Cypriot or foreign, and gold bullion worth CP 7,300 (approximately U.S. \$18,250) or more. The Central Bank has the authority to revise this amount. On June 15 2007, EU Directive 1889/2005, went into effect. As a result, for currency worth €10,000 (U.S. \$14,620) or more, Cyprus regulates cash transactions for travelers entering its borders from countries outside the EU.

Cyprus is currently in the process of passing legislation entitled “Law for the Prevention and Suppression of Money Laundering Activities,” which was expected to pass without significant changes before the end of 2007. This legislation will consolidate and supersede existing legislation. When enacted, the draft law will encompass all recent FATF and MONEYVAL recommendations, and revises Cyprus’ AML legislation, to harmonize it with the EU’s Third AML Directive. This Directive mandated implementation by December 15, 2007. The new law provides much stricter administrative fines for noncompliance, i.e., from the current €5,130 (U.S. \$7,500) to €200,000 (U.S. \$292,400) and generally raises Cyprus’ AML standards.

The draft law also addresses: enhanced due diligence extending coverage of “politically-exposed persons” (PEPs), cross-border transactions, and transactions with customers not physically present or on behalf of third parties. The law introduces simplified due diligence for certain persons or entities deemed to be low risk as well as requirements for Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU), and other supervisory authorities to collect statistical data. MOKAS must provide banks and other obligated entities with feedback in response to any STR submission. The law criminalizes the general collection of funds with the knowledge that terrorists or terrorist groups would use them for any purpose (i.e., not just for violent acts); and terrorism finance is explicitly covered by the new law (although already considered a predicate offense under existing legislation).

A second draft law, expected to pass by early 2008, regulates trust and company service providers (other than accountants and lawyers), bringing them under the supervisory authority of the Central Bank. As soon as these laws go into effect, the supervisory authorities will issue revised directives.

In October 2006, the IMF released a detailed assessment of the “Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation.” The report noted that the Cyprus Securities and Exchange Commission (SEC) was legally unable to cooperate with foreign regulators if the SEC did not have a direct interest and that the SEC had difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The report also noted

that commitments emerging from EU accession had “placed stress on the skills and resources” of the staff of the Co-operative Societies Supervision and Development Authority (CSSDA) and the Insurance Superintendent. The SEC has drafted amending legislation to resolve these issues, expected to pass by early 2008.

In recent years the Central Bank has introduced regulations aimed at strengthening AML vigilance in the banking sector. Among other requirements, banks must ascertain the identities of the natural persons who are the “principal/ultimate” beneficial owners of all legal entities; adhere to the October 2001 paper of the Basel Committee on Banking Supervision on “Customer Due Diligence for Banks”; and pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as deficient in their AML regime, particularly concerning counter-terror financing (CTF).

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding 10,000 Cypriot pounds (approximately U.S. \$22,000 in local currency) or approximately U.S. \$10,000 in foreign currency. Bank employees must report all suspicious transactions to the bank’s compliance officer, who determines whether to forward a report to the Cypriot FIU for investigation. Banks retain reports not forwarded to the FIU, which the Central Bank audits as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious transaction reports (STRs) submitted to the compliance officer and the number forwarded by the compliance officer to the FIU. Bank officials may be held personally liable if their institutions launder money. Cypriot law partially protects reporting individuals with respect to their cooperation with law enforcement but does not clearly absolve a reporting institution or its personnel from complete criminal or civil liability. Banks must retain client identification data, transaction records, and business correspondence for five years.

Central Bank money laundering directives place additional obligations on banks, including requirements on customer acceptance policy; and updating customers’ identification data and business profiles. Banks must have computerized risk management systems to verify whether a customer constitutes a PEP; provide full details on any customer sending an electronic transfer in excess of U.S. \$1,000; and have adequate management information systems for on-line monitoring of customers’ accounts and transactions. Cypriot banks typically use electronic risk management systems to target transactions to and from high-risk countries, as well as high-risk customers. Since the expiration of Cyprus’ Exchange Control Law, the Central Bank no longer reviews foreign investment applications for nonEU residents. Since January 1, 2007, Cyprus has begun implementing EU Directive 1781/2006 (“Information on the Payer Accompanying Transfers of Funds”), which requires full disclosure of details for electronic fund transfers in excess of €1,000 (U.S. \$1,462).

The Central Bank also requires compliance officers to file annual reports outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank has the authority to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus’ “know-your-customer” rules, which form the basic part of Cyprus’ AML system. As a result of the approval, banks in Cyprus that acquire United States securities on behalf of their customers may enter into a “withholding agreement” with the IRS and become qualified intermediaries.

The Prevention and Suppression of Money Laundering Activities Law mandated the establishment of the Unit for Combating Money Laundering (MOKAS), the Cypriot financial intelligence unit (FIU). MOKAS is responsible for receiving and analyzing STRs and for conducting money laundering investigations. A representative of the Attorney General’s Office heads the unit. All banks and nonbank financial institutions, insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in a

significant increase in the number of STRs being filed. Between January 1 and November 19, 2007, MOKAS received 160 STRs. In the same interval, MOKAS received 261 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS cooperates closely with the U.S. in money laundering investigations.

Money laundering is an autonomous crime in Cyprus. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. MOKAS has the power to administratively suspend financial transactions for an unspecified period of time. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a preliminary stage of an investigation. MOKAS has issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have resulted in the closure of dormant bank accounts. MOKAS conducts AML training for Cypriot police officers, bankers, accountants, and other financial professionals, and, in conjunction with the Central Bank of Cyprus, for bankers.

During the interval from January 1 through November 19, 2007, MOKAS opened 447 cases and closed 150. Since 2000, there have been 13 prosecutions for money laundering, one of which took place in 2007. Of the 13 prosecutions, eight have resulted in convictions. In 2007, MOKAS issued one confiscation order for a total of approximately \$10.5 million. A number of other cases are pending.

Sections 4 and 8 of the Ratification Law 29 (III) of 2001 criminalize terrorist financing. The implementing legislation amends the AML law to criminalize the collection of funds in the knowledge that these would be used by terrorists or terrorist groups for violent acts. The parliament passed an amendment to the implementing legislation in July 2005 eliminating a loophole that had inadvertently excused Cypriot nationals operating in Cyprus from prosecution for terrorism finance offenses. MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs or the U.S. Treasury Department as a terrorist or a terrorist organization.

Under a standing instruction, the Central Bank automatically issues a “search and freeze” order for accounts matching the name of any entity or group designated by the UN 1267 Sanctions Committee or the EU Clearinghouse as a terrorist or terrorist organization. If a financial institution finds matching accounts, it will immediately freeze the accounts and inform the Central Bank. As of November 2007, no bank has reported holding a matching account. When FIUs or governments—not the UN or the EU Clearinghouse—designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contacts commercial banks directly to investigate. To date, none of these checks have revealed anything suspicious. The lawyers’ and accountants’ associations cooperate closely with MOKAS and the Central Bank. Cyprus cooperates with the United States to investigate terrorist financing. MOKAS reports that no terrorist assets have been found in Cyprus to date and thus there have been no terrorist finance prosecutions or freezing of terrorist assets. In 2006, there was one investigation for terrorist financing involving four persons.

Cyprus believes that its existing legal structure is adequate to address money laundering through alternative remittance systems such as hawala. Cypriot authorities maintain that there is no evidence that alternative remittance systems such as hawala operate in Cyprus. Cyprus licenses charitable organizations, which must submit copies of their organizing documents and annual statements of account to the government. The majority of charities registered in Cyprus are reportedly domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Cyprus has signed, but not ratified, the UN Convention Against Corruption. Cyprus is a member of MONEYVAL the FATF-style regional body for Council of Europe member states. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs)

with 17 FIUs, although Cypriot law allows MOKAS to share information with other FIUs without benefit of an MOU. A mutual legal assistance treaty between Cyprus and the United States entered into force September 18, 2002.

Cyprus has put in place a comprehensive AML/CTF regime, which it continues to upgrade. Cyprus should ensure not only the passage, but also the full implementation, of the two laws that will tighten the current regime requirements. Cyprus should ensure that it is able to implement the law criminalizing the collection of funds with the knowledge that they will be used by terrorists or terrorist groups for any purpose, not only to commit terrorist or violent acts. Cyprus should enact provisions that allow for civil forfeiture of assets in the future.

Area Administered by Turkish Cypriots. The Turkish Cypriot community continues to lack the legal and institutional framework necessary to provide effective protection against the risks of money laundering. There are currently 24 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 14 banks and approximately 50 companies. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The “Central Bank” audits the offshore entities, which must submit an annual report on their activities. However, the “Central Bank” has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the “Ministry of Finance” performs this function. A new law restricts the granting of new bank licenses to only those banks with licenses in an OECD country or a country with “friendly relations” with the “TRNC.” A new law to more closely regulate offshore banks is pending in “parliament.”

It is thought that the 18 essentially unregulated and primarily Turkish-mainland owned casinos and the 14 offshore banks are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks on applicants are minimal. A significant portion of the funds generated by these casinos reportedly change hands in Turkey without ever entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Another area of concern is the approximately five hundred “finance institutions” operating in the area that extend credit and give loans. Although they must register with the “Office of the Registrar of Companies,” they remain unregulated. Some of these companies are owned by banks and others by auto dealers. Recent years have seen a large increase in the number of sport betting halls, which are licensed by the “Office of the Prime Minister.” There are currently five companies operating in this sector, with a total of 30 outlets. Four of the companies also accept bets over the Internet. Turkish Cypriot authorities deported one prominent Turkish organized crime figure, Yasar Oz, following a December 19, 2006 shootout at the Grand Ruby Casino that left two dead. As a result of this incident, the Turkish Cypriot authorities arrested seven individuals, closed the Grand Ruby and Denizkizi Casinos and deported much of their staff. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey.

The fact that the “TRNC” is recognized only by Turkey limits the ability of Turkish Cypriot authorities to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any regional FATF-style organization and thus is not subject to any peer evaluations. In 2007, FATF conducted an informal review and found numerous shortcomings in AML laws and regulations as well as insufficient resources devoted to the effort. Turkish Cypriot officials objected to the conclusions.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury’s FinCEN, pursuant to Section 311 of the USA PATRIOT Act, found First Merchant Bank to be of primary money laundering concern based on a number of factors. These factors, included that it is licensed as an offshore bank in a jurisdiction with inadequate AML controls, particularly those applicable to its offshore sector; and that it is involved in the marketing and sale of fraudulent financial products and services. Other factors point to its use as a conduit for the laundering of

fraudulently obtained funds; and its apparent use to launder criminal proceeds by the individuals who own, control, and operate First Merchant Bank—individuals with links to organized crime. In December 2006, the Turkish Cypriot administration ordered First Merchant Bank to cease its operations due to violations of the Turkish Cypriot “Offshore Banking Law.” The bank is now only permitted to perform activities associated with closing the Bank such as the payment and collection of outstanding debts.

Turkish Cypriot authorities have begun taking limited steps to address the risk of financial crime, including enacting an anti-money laundering law (AMLL) for the area. The law aims to reduce the number of cash transactions in the area administered by Turkish Cypriots, as well as improve the tracking of any transactions above U.S. \$10,000. Under the AMLL, banks must report to the “Central Bank” any electronic transfers of funds in excess of U.S. \$100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over U.S. \$20,000 and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports (STRs) to a five-member “Anti-Money Laundering Committee (AMLC)” which decides whether to refer suspicious cases to the “police” and the “attorney general’s office” for further investigation. The five-member committee is composed of representatives of the “police,” “customs,” the “Central Bank,” and the “Ministry of Finance.” However, the AMLL has never been fully implemented or enforced.

In 2005, the “AMLC,” which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file STRs. The committee has reportedly referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals for money laundering, although one foreign bank owner suspected of having ties to organized crime was successfully extradited. There are significant concerns that law enforcement and judicial authorities lack the technical skills needed to investigate and prosecute financial crimes. The “AMLC” also complains that since foreign jurisdictions will not cooperate with them by providing evidence or appearing to testify, they have difficulty presenting cases to their court system.

Although the AMLL prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than U.S. \$10,000 in currency without prior “Central Bank” authorization, “Central Bank” officials note that this law is difficult to enforce. This is particularly true given the large volume of travelers to and from Turkey, especially since Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The “Ministries of Finance, Economy and Tourism” are drafting several new AML laws that they claim will, among other things, establish an FIU and provide for better regulation of casinos, currency exchange houses, and both onshore and offshore banks. Turkish Cypriot authorities have committed to ensuring that the new legislation meets international standards. However, it is unclear if or when the new legislation will be adopted, and if it is adopted, whether it will ever be fully implemented and enforced. Work on the new bills has been ongoing for more than three years. Turkish Cypriot officials have promised FATF that the laws will pass in 2007, after which the European Commission plans to help with their implementation through selected training and funding.

The Turkish Cypriot AMLL provides better banking regulations than were previously in force, but as an AML tool it is far from adequate, and without ongoing enforcement, cannot meet its objectives. A major weakness continues to be the many casinos, where a lack of resources and expertise leave that

area essentially unregulated and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to enact a new anti-money laundering law, establish a strong, functioning “financial intelligence unit”, and adopt and implement a strong regulatory environment for all obliged institutions, in particular casinos, money exchange houses, and entities in the offshore sector. Turkish Cypriot authorities should take steps to enhance the expertise of members of the enforcement, regulatory, and financial communities with an objective of better regulatory guidance, the more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions. Passage of new laws and willingness to cooperate with foreign experts for implementation will be the early tests of a change in approach to these issues.

Czech Republic

The Czech Republic is one of the most stable and prosperous of the post-Communist states of Central and Eastern Europe. However, the Czech Republic’s central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics trafficking, trafficking in persons, fraud, counterfeit goods, embezzlement and smuggling) remain the primary source of laundered assets in the country, Czech officials and media outlets have voiced increasing concern about the ability of extremist groups and terrorists to launder or remit money within the country. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity, most commonly by means of financial transfers through the Czech Republic. Banks, currency exchanges, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds. Currency exchanges in the capital and border regions are also considered to be a major problem.

The growth of the Czech Republic economy between 2000 and 2007 was supported by exports to the European Union (EU), primarily to Germany. However, despite the progressive development of modern payments techniques, the economy is still heavily cashed-based. The Czech Republic decided to adopt the single European currency (euro) in connection with its accession to the EU in 2004, and in July 2007 the Organizational Committee of National Coordination Group published “The National Changeover Plan for the Czech Republic,” which covers the technical, legislative and organizational preparation for the future introduction of the euro in Czech Republic.

Major sources of criminal proceeds include criminal offenses against property, insurance fraud, and credit fraud. Connections between organized crime and money laundering have been observed mainly in relation to activities of foreign groups, in particular from the former Soviet republics, the Balkan region, and Asia. The Czech Republic is also vulnerable to other illicit financial activities conducted through credit and loan services, money remittances (particularly in connection with the Asian community), and illegal foreign exchange business.

The Government of the Czech Republic (GOCR) first criminalized money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002 amendment to the Criminal Code introduces a new independent offense called “Legalization of Proceeds from Crime.” This offense has a wider scope than previous provisions and enables prosecution for laundering one’s own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulates punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and calls for the forfeiture of assets associated with money laundering. Despite some improvements, the criminalization of money laundering under Section 252a (“Legalization of Proceeds from Criminal Activity”) of the Criminal Code still does not contain a broad definition and coverage of money laundering. To date, Section

252a has mostly been applied to criminal offenses that have more to do with stolen goods than with the laundering proceeds.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. The Anti-Money Laundering (AML) Act, which provides for the general preventive framework, was adopted in 1996 and covered only the banking sector. It has been amended several times and to comply with EU requirements. The law now requires a wide range of financial institutions, as well as attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in financial transactions, to report all suspicious transactions to the Ministry of Finance's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU). Suspicious transactions exceeding 15,000 euros (approximately U.S. \$22,140) must be reported, and those exceeding 1,000 euros (approximately U.S. \$1,476) must be identified internally.

The GOCR recently approved a new draft law on "Measures against Legalization of Proceeds from Criminal Activity and Terrorism Financing." This proposal implements the EU's Third Money Laundering Directive. Legislative approval by December 15, 2007, as requested by the EU, is expected. In connection with this effort, the Czech National Bank is preparing an amendment to the foreign currency law that would introduce new regulations and licensing requirements for currency exchanges.

The Law on International Sanctions that came into force in April 2006 also represents progress by the GOCR. Under this law, the Ministry of Finance has the authority to fine institutions for failure to report accounts or other assets belonging to individuals, organizations, or countries, on which international sanctions have been imposed, or those not fulfilling other obligations set by international regulations. Earlier laws restricting financial cooperation with the Taliban (2000) and Iraq (2005) were replaced by the Law on International Sanctions.

The Czech Republic still has more than 2.6 million anonymous deposit passbooks containing 3.9 billion crowns (approximately U.S. \$200 million). Due to ongoing criticism, the Czech Republic introduced legislation in 2000 prohibiting new anonymous passbook accounts. In 2002 the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002. In principle, bearer passbooks will be completely phased out by 2012. While account holders can still withdraw money from the accounts for another few years, the accounts do not earn interest and cannot accept deposits. In 2007, approximately 350 million crowns (approximately \$18 million) were withdrawn from these accounts. Although in general the customer identification procedures are mostly in place, full customer due diligence (CDD) requirements should be introduced in the AML Act with appropriate guidance.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the AML Act, anyone entering or leaving the Czech Republic with more than 10,000 euros (approximately U.S. \$14,750) in cash, traveler's checks, or other monetary instruments must make a declaration to customs officials, who are required to forward the information to the FAU. Similar reporting requirements apply to anyone seeking to mail the same amount in cash to or from the country. In practice, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult.

The FAU was established in July 1996 as an administrative FIU under the umbrella of the Ministry of Finance. It has overall supervisory competence to ensure the implementation of the AML Act by all obliged entities. Since 2000 financial institutions have been required to report all suspicious transactions to the FAU. The FAU is authorized to share all information with the Czech Intelligence

Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the Czech Police, Customs, and counterparts abroad. The GOCR expects that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government.

The FAU is charged with reviewing suspicious transaction reports (STRs) filed by police agencies, financial, and other institutions. It is also charged with uncovering cases of tax evasion, which is a widespread problem in the Czech Republic. The FAU has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities remain with the Czech National Police Unit for Combating Corruption and Financial Crimes (UOKFK) or other Czech National Police bodies. The FAU's work covers only a relatively small segment of total financial activity within the Czech Republic. Since April 2006, the FAU has had the power to fine financial institutions that fail to report accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed.

The UOKFK has primary responsibility for all financial crime and corruption cases. Following the dissolution of the specialized Financial Police on January 1, 2007, the unit became the main law enforcement counterpart to the FAU and is responsible for investigations of terrorist financing cases. Following the abolition of the Financial Police, the UOKFK took over all of its ongoing cases, but the pace of investigations has slowed.

The number of STRs transmitted to the FAU has been growing. There were 3,404 suspicious transactions reported in 2005 and 3,480 in 2006. From January through October 2007, there were 1,729 reports of suspicious transactions. This upward trend is interpreted as evidence of the active participation of concerned entities in the anti-money laundering regime. Conversely, the number of inquiries evaluated and forwarded to law enforcement bodies have decreased compared to 2005. In 2005, the FAU forwarded 208 reports to the police and only 137 in 2006. From January through October 2007, the number of reports forwarded to the police was 82; in 25 cases, the payments were temporarily frozen. The abolition of the Financial Police and the transfer of its cases to the Unit Combating Corruption and Financial Crimes caused temporary difficulties in communication between the FAU and the Police. It is not clear whether every case transferred to law enforcement was investigated. Cooperation with foreign counterparts remains good. In 2005, the FAU received 130 assistance requests from abroad and sent 69 requests abroad. In 2006, it received 128 and sent 77. During the first nine months of 2007, the FAU received 102 requests and sent out 49 requests.

From January to June 2007, the Police investigated eight individuals, but did not seize any related funds. This is a significant decrease from 2006, when the police investigated 11 offenders and seized 373 million crowns (approximately \$20 million). The decrease can be partially explained by the abolition of the specialized Financial Police.

The Czech Republic saw its first convictions of individuals attempting to legalize proceeds from crime only in 2004. In 2005, there were 23 alleged offenders prosecuted and three were convicted. In 2006, there were 33 were prosecuted, and five convicted. In the first half of 2007, only six people were prosecuted and two convicted. The sentences were low and included suspended sentences or fines. An ongoing issue in criminal prosecutions is that law enforcement agencies must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has increased in recent years, both the FAU and the Police face staffing challenges. The Financial Action Task Force (FATF) and the Council of Europe's FATF-style regional body (MONEYVAL) have both emphasized the need for the Czech Republic to increase the FAU's staff. Given the scope of its responsibilities, the FAU remains a relatively small organization. The Police face even bigger challenges due to recent changes in police retirement rules and the perceived lack of

political support for independent police work. Many senior and experienced police officers are reportedly leaving or are considering early retirement. These departures will affect not only the UOKFK, but the Organized Crime Unit and other critical police organizations as well. The dissolution of the Financial Police, which was created in 2004 in response to EU recommendations and had a good track record of investigating and prosecuting money laundering and terrorist finance cases, has also had a negative impact on police work on financial crimes.

Czech laws facilitate the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to 72 hours to give the FAU sufficient time to investigate whether there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. If sufficient evidence of criminal activity exists, the case is forwarded to UOKFK, which has another three days to gather the necessary evidence. If the UOKFK is able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72-hour time limit, the UOKFK fails to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by suspected terrorists and terrorist organizations, or by other individuals and organizations covered under the Law on International Sanctions.

Although Czech law authorizes officials to use asset forfeiture, it is still not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's consent) to freeze an account or assets if evidence indicates that the contents were used or will be used to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours must inform the prosecutor, who then confirms the freeze or releases the funds. An amendment to the 2004 Law on the Administration of Asset Forfeiture in Criminal Procedure implemented provisions and responsibilities overseeing the administration and storage of seized property and appoints the police as administrators of seized assets.

A 2006 amendment to the Czech Criminal Procedure Code and Penal Code brought several positive changes to the asset forfeiture and seizure law. The law, as amended, now allows for the freezing and confiscation of the value of any asset (including immovable assets) and is not limited to property. These provisions allow the police and prosecutors to seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute asset values as well as asset values not belonging to the criminal.

The National Drug Headquarters (NDH) cooperates with the UOKFK on drug-related cases. However, as a result of the abolition of the Financial Police the NDH conducts its basic financial investigations alone and, if needed, contacts the UOKFK. In the first ten months of 2007, the NDH confiscated 1.9 million crowns (approximately U.S. \$108,000), 44 thousand euros (approximately U.S. \$65,000), and other assets valued at 1.8 million crowns (approximately U.S. \$103,000).

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. A penalty of up to 15 years' imprisonment can be imposed on those who support terrorists financially, materially, or by other means. In addition to reporting all suspicious transactions possibly linked to money laundering, concerned institutions are now required to report all transactions suspected of being tied to terrorist financing. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list.

The Czech Republic ratified the UN International Convention for the Suppression of the Financing of Terrorism in October 2005. Subsequently, the GOCR adopted the National Action Plan for the Fight against Terrorism for 2005-2007. This document covers topics such as police work and cooperation,

protection of security interests, enhancement of security standards, and customs issues. The fight against terrorist financing is one of the major priorities contained in the plan.

Although the terrorist finance threat in the Czech Republic is considered to be modest, some law enforcement officials believe that the presence of third-country remuneration networks operating in the country (“hawala” shops) could translate into a greater possibility of financing terrorist activities. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. A governmental body called the Clearinghouse was established in 2002 to streamline the collection of information from institutions to enhance cooperation and response to a terrorist threat. The Clearinghouse meets only in cases of necessity. It has not met thus far in 2007. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts, and adoption of the Law International Sanctions has made their work easier. Several cases have been detected, and payments to suspected organizations were not permitted. No sanctions have been imposed.

The Czech Republic has signed memoranda of understanding on information exchange with 23 countries, and, most recently, signed a new agreement with Paraguay. The Czech Republic formalized an agreement with Europol in 2002. The FAU has been a member of the Egmont Group since 1997 and is authorized to cooperate and share information with all of its international counterparts, including those that are not part of the Egmont Group. The Czech Republic participates in MONEYVAL. The most recent mutual evaluation of Czech Republic was conducted by the MONEYVAL in 2006. The mutual evaluation report (MER) was adopted by the MONEYVAL at its 24th plenary meeting in December 2007.

The Czech Republic is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Czech Republic is also a party to the World Customs Organization’s Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In May 2006, the United States and the Czech Republic signed a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects; however, these instruments have not yet been ratified.

The Government of the Czech Republic has made progress in its efforts to strengthen its money laundering regime. The GOCR cooperates to a large extent with foreign counterparts in the field of anti-money laundering and counter-terrorist financing. However, the incomplete Czech legal framework on seizure and confiscation is a major limitation to its international cooperation, and its staffing problems could be an obstacle to timely and effective collaboration. Czech authorities are using a risk-based approach when determining priorities and imposing obligations on obliged entities. However, there is a tendency to rely on assumptions rather than on assessments, and as a result there is a lack of unanimity on sectors exposed to and used for money laundering purposes. The Czech Republic should approve already-drafted amendments to its existing money laundering legislation by to implement the European Union’s Third Money Laundering Directive. The GOCR should also ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.